FSVS
SIGNALING PLAN –
INTEROPERABLE MODES

Prepared For:

National Security Agency
9800 Savage Road
Fort George G. Meade, MD 20755-6000

Prepared By:

GTE

Electronic Defense Communications Directorate
GTE Government Systems Corporation
100 First Avenue
Waltham, MA 02154

LIST OF ACRONYMS (Cont.)

ACRONYM	TITLE
FSVS	Future Secure Voice System
GNS	Go Non-Secure
GPA	Modem Scrambler Designation
GPC	Modem Scrambler Designation
GW	Gateway
HDX	Half Duplex
Hz	Hertz
KG	Key Generator
KMC	Key Management Center
LIT	Line Interface Terminal
LPC	Linear Predictive Code
LTC	Local Terminal Cipher message
LRCM	Local Random Component Message
mA	milliAmpere
MID	Message Identifier
ms	millisecond
OOS	Out of Sync
POTS	Plain Old Telephone Service
RCC	Random Component Cipher message
RLS	Release
RRCC	Remote Random Component Cipher message
RTC	Remote Terminal Cipher message
SCR1	Scrambled Ones (message pattern)
SD	Secure Dial
sec	second
SOM	Start of Message
STU	Secure Telephone Unit
TC	Terminal Cipher message
UDM	Universal Decrypt Modulus
VOX	Voice Operated Exchange

APPENDIX A
LIST OF ACRONYMS

ACRONYM	TITLE
AC	Alternating Current
BERT	Bit Error Rate Test
bps	bits per second
CAP/SV	Capability/Status Vector
CCITT	International Consultative Committee on Telegraphy and Telephony
CIK	Crypto Ignition Key
CKL	Compromised Key List
CIM	Compromise Information Message
COMSEC	Communications Security
CS	Crypto Synchronization message, also Clear-to-Send Digital Interface as defined in RS-449
DC	Direct Current
dibit	two bit Sequence
DP	Dial Pulse
DSN	Defense Switched Network
DTMF	Dual Tone Multifrequency
EC	Echo Canceller
EIA	Electronic Industries Association
EOM	End of Message
ESC	Escape
ESD	Echo Suppressor Disable
ESCD	Echo Suppressor/Canceller Disable
FCC	Federal Communications Commission
FDX	Full Duplex
FF	FIREFLY
FSTS	Federal Secure Telephone System

Table of Contents

4.4.4 Secure Bit Error Rate Test (BERT)

The Secure Bit Error Rate Test mode has been included as a discretionary option for the STU-III terminal. The STU-III will only be able to enter this mode if the far end terminal has indicated, in the CAP/SV, that it can receive BERT information. In the full duplex BERT mode, each STU-III will transmit encrypted zeros as long as the mode is active. The BERT signaling in the half duplex mode provides for the transmission of encrypted zeros for a nominal ten seconds. There are no signaling interoperability requirements imposed on the receive processing of the resulting incoming information.

4.4.5 KMC Rekey Message

The format for the Rekey messages is defined in FSVS-220, Section 2.6.8.5.

4.4.6 Rekey ACK

The format for the Rekey ACK message is defined in FSVS-220, Section 2.6.8.6.

4.4.7 Compromised Key List (CKL)

The format for the CKL message is defined in FSVS-220, Section 2.6.8.7.

4.4.8 CKL ACK

The format for the CKL ACK message is defined in FSVS-220, Section 2.6.8.8.

Table of Contents (Cont.)

Table 4-4. Secure Dialing BCH Block Format

Bits	Field
255-252	1st digit code
251-248	2nd digit code
247-244	3rd digit code
. . .	
131-128	32nd digit code
127-125	reserved
124- 1	BCH parity
0	reserved

Table of Contents (Cont.)

Table 4-3. Secure Dialing Digit Codes

Keypad Digit	Function	Transmitted Code (bits)
-	Null	0000
1	Digit 1	0001
2	Digit 2	0010
3	Digit 3	0011
4	Digit 4	0100
5	Digit 5	0101
6	Digit 6	0110
7	Digit 7	0111
8	Digit 8	1000
9	Digit 9	1001
0	Digit 0	1010
*	*	1011
#	#	1100
-	Unassigned	1101
P	Precedence	1110, 0001
I	Immediate	1110, 0010 Note 1
F	Flash	1110, 0011
FO	Flash Override	1110, 0100
-	Unassigned	1111

Note 1: All eight bits are transmitted when any one of the priority digits are depressed.

Table of Contents (Cont.)

These options differ from data bearing messages defined above in that they follow a Crypto Sync/Filler/Start sequence, they are encrypted prior to transmission and they are not scrambled. This section describes the transmission formats for each traffic option.

4.4.1 Secure Voice

The STU-III shall be capable of digitizing speech at a rate that can be transmitted in a full or half duplex fashion over the standard telephone networks. The present interoperable signaling mode only includes 2400 bps operation.

4.4.2 Secure Data

The STU-III shall be capable of transmitting synchronous data securely at 2400 bps. The STU-III may optionally be capable of transmitting BCH coded 1200 bps asynchronous or full rate 1200 bps asynchronous data over the 2400 bps synchronous link. The STU-III may optionally be capable of transmitting 2400 bps asynchronous data over the 2400 bps synchronous link. The STU-III will ensure that all data received from the serial data interface are transmitted in the order received from the data device.

4.4.3 Secure Dial

The secure dialing option is used to transfer dialing information entered by the subscriber to a far-end STU-III. The STU-III will only be able to enter this mode if the far end terminal is capable of receiving secure dialed digits as indicated in the CAP/SV message. Up to 32 dialed digits (see Table 4-3), four bits per digit (except for priority keys which require eight bits per digit), will comprise a BCH coded traffic block. The 32 dialing codes are grouped into a BCH coded block after the codes themselves are first encrypted. The actual BCH-coded message block will include the dial code information as defined in Table 4-4. The STU-III may send as many BCH blocks as necessary to transfer the dialing information. The STU-III shall append the null code to complete the final BCH block if there are less than 32 dialing codes to transmit.

Table of Contents (Cont.)

4.2.6.2 Retrain NACK

The Retrain NACK is a non-data bearing message that is transmitted in response to a "Retrain Request" to indicate that the responding terminal is not configured to honor the retraining request. This message is preceded by an Escape sequence in the full duplex mode.

4.3 DATA BEARING MESSAGES

The format of data bearing messages is defined in FSVS-220, Section 2.6.8.

4.3.1 Cryptosynchronization

The format of cryptosynchronization messages is defined in FSVS-220, Section 2.6.8.9.

4.3.2 Capability/Status Vector (CAP/SV) Message

The format for the CAP/SV message is defined in FSVS-220, Section 2.6.8.1.

4.3.3 Terminal Cipher Message (TC) Message

The format for the TC message is defined in FSVS-220, Section 2.6.8.2.

4.3.4 Random Component Cipher (RCC)

The format for the RCC message is defined in FSVS-220, Section 2.6.8.3.

4.4 SECURE TRAFFIC FORMATS

There are eight types of secure traffic presently defined for the STU-III interoperable mode. These are defined below for Secure Voice, Secure Data, Secure Bit Error Rate Test (BERT) and Secure Dialing, and in the classified attachment to FSVS-220 for KMC Rekey and CKL messages.

List of Illustrations

4.2.4 Idle

This message is transmitted at nominal three second intervals in the (half-rate) HDX mode by the KMC STU-III terminal to indicate to the STU-III that the channel is still functioning properly and that the KMC intends to continue transmission.

4.2.5 Retrain Request

This non-data bearing message is used to indicate that the user wants to terminate the current modulation format and retrain and modem to the same or to a new format while remaining in the secure mode of operation. This message is preceded by an Escape sequence in the full duplex mode.

This message shall only be used by and transmitted to terminals which have transmitted a CAP Version No. of greater than or equal to one in the capabilities portion of the CAP/SV message. Other terminals receiving this message shall respond with a Failed Call sequence.

4.2.6 Retrain NACK and ACK Message

These Retrain ACK (RTRA) and Retrain NACK (RTRN) message shall only be used by and transmitted to terminals which have transmitted a CAP Version No. of greater than or equal to one in the capabilities portion of the CAP/SV message. Other terminals receiving these messages shall respond with a Failed Call message.

4.2.6.1 Retrain ACK

The Retrain ACK (RTRA) is a non-data bearing message that is transmitted in response to a "Retrain Request" to indicate that the responding terminal accepts the retrain request. This message is transmitted only in half duplex.

List of Illustrations (Cont.)

Figure	Title	Page

Table 4-2. Non-Data Bearing Message Identifiers

Message	MID
Release	00130000
User Abort	00200000
Failed Call	20210000
Restart Failed Call	22100000
Idle	01110000
Retrain Request	01210000
Retrain ACK	32110000
Retrain NACK	01220000
Reserved for Motorola	22010000
Reserved for Motorola	22020000
Reserved for RCA	01120000

List of Illustrations (Cont.)

The description of each non-data bearing message is provided below with a listing of the MID assignments in Table 4-2.

4.2.1 Release

The Release message is transmitted to indicate that a terminal has gone on hook. In full duplex mode, Escape always precedes the SOM/Release sequence. In half duplex mode the SOM/Release sequence is not preceded by the Escape sequence.

4.2.2 User Abort

The User Abort message is transmitted to indicate that a user wants to transition from the secure mode of operation to the analog non-secure mode of operation. This message is also preceded by Escape in the full duplex mode only.

4.2.3 Failed Call Messages

4.2.3 1 Failed Call

The Failed Call message indicates that the STU-III has detected a signaling failure or procedural problem which prohibits continuation/recovery of the secure call or call set up. Both users have the option of going back to analog traffic by activating the non-secure control. This message is also preceded by Escape in the full duplex mode only.

4.2.3.2 Restart Failed Call

This message is transmitted only in the full duplex V.32 mode of operation. It is used to signal a failure during call setup coupled with a request to restart call setup in the 2400 bps interoperable mode.

List of Illustrations (Cont.)

2) In the half duplex mode, all non-data bearing messages are preceded by P1800, the 3202 transition dibit sequence, SCR1 (64 bits), and the 64-bit SOM. The end of a transmission is indicated by the 256 bit EOM message (same bit pattern as Escape),

3) In the half duplex mode, the Escape sequence is not used as a flag for a change in signaling since every transmission contains either another CS message and the associated traffic, or it contains one of the non-data bearing messages to indicate a non-traffic transmission,

4) The MID and the data portion of non-data bearing messages are scrambled (see Chapter 3 for the scrambler characteristics).

The non-data bearing messages contain an 8 dibit Message Identifier Field (MID), which uniquely identifies the purpose of the message in the first four dibits and the number of blocks in the remainder of the message in the next four dibits, followed by 56 dibits all set to zero. This 64 dibit message is transmitted in a BCH-coded 128 dibit block with the resulting structure:

MID 8 Dibits	56 dibits	(zeros)	3 bits (Reserved)	62 parity dibits	1 bit (Reserved)

The first four bits of the MID patterns have been chosen to provide a minimum Hamming distance of 2 (two) between any two MIDs (the first four dibits).

The patterns are generated by specifying that the MIDs have odd parity and use the most significant bit as the parity bit. The second 8 bits are designated as the block count (# of blocks following the first BCH block). For non-data bearing messages, the second four dibits of the MID are all zero since there are no blocks following the non-data bearing message block.

List of Tables

ESCAPE is always followed immediately by SOM: that is, the ESCAPE is always followed immediately by the MSB of SOM. Escape is used to signify any of the following:

1) One or both of the terminals going on hook in full duplex mode; precedes RELEASE,
2) One or both of the terminals declaring any mode change (e.g., voice/data, data/voice transition) in full duplex mode,
3) Out of sync condition in full duplex mode,
4) Abort or failed call conditions in full duplex mode.

4.1.7 End of Message (EOM)

EOM is a 128 dibit long supervisory message. It is the same dibit sequence as the Escape pattern (paragraph 4.1.6) and is used in Half Duplex mode to notify the terminal of the end of a message transmission. EOM is always sent as a complete message and is never truncated.

4.2 NON-DATA BEARING MESSAGES

All non-data bearing (control) messages have a common format. The message formats for non-data bearing messages are presented in this section without the half duplex preamble, SOM, filler frames, full duplex escape sequences, and half duplex EOM flag to prevent confusion between actual messages and transmission overhead or signaling overhead.

The following rules apply to non-data bearing and "not encrypted" messages:

1) In the full duplex mode, any change in signaling (i.e., from secure traffic) is indicated by the 256-bit Escape sequence followed by a SOM and the appropriate message,

SECTION 1
INTRODUCTION

This document specifies the common interoperable modes of signaling required of all system elements in the Future Secure Voice System (FSVS). It describes the signaling between STU-IIIs in the common interoperable modes, between STU-IIIs and the KMC, and between STU-IIIs and other network elements.

The FSVS Signaling design has been developed to provide reliable and responsive call processing consistent with the requirements and goals of the overall FSVS program. This document reflects a baseline standard for the FSVS signaling, with provisions for expansion to allow different manufacturers to incorporate unique features into their STU-III designs and to accommodate future growth while ensuring interoperability of all FSVS network elements.

This document is intended to define functional requirements of the STU-III as they relate to signaling. It is not intended to force selection of components or technologies, nor force specific implementations. Specific components, technologies and implementations which may be described, are solely for the purpose of clarity and should not be considered a design restriction.

1.1 STRUCTURE OF PLAN

The signaling design is structured in three hierarchical layers, each performing specific functions and services, building on those performed at layers below. The three layers are:

- Signaling Protocols — The actual sequences which are followed during clear and secure (voice and data) call set-up and traffic.

4.1.4.3 Terminology

The terms SOM(C), START(C), SOM(A), and START(A) will be used to refer specifically to the patterns identified above. The terms SOM and START (or ST) will be used to refer to one of the two patterns when the context does not require greater precision, and may also be used to refer to the specific patterns when it is clear from the context which is required. The acronyms ST, ST(A), ST(C) will also signify START, START(A), AND START(C), respectively.

4.1.5 Filler

Filler is a 32 dibit long supervisory message. It is used to separate messages to allow for variations in BCH coding/decoding and Firefly coding/decoding times. It is a 64 bit sequence of all zeroes. Filler is always sent as a complete 64 bit message and is never truncated. Filler blocks are always scrambled with a continuation of the scrambling sequence used to scramble the preceding message. Filler is never BCH coded and is never encrypted.

4.1.6 Escape (ESC)

Escape is a 128 dibit long supervisory message. It is generated from a 127 bit prime number sequence repeated twice and padded with the first two bits of the sequence to become a 128 dibit message. It is used to notify a terminal of a change in operation in full duplex mode. It is always sent as a complete message and is never truncated. Escape is shown in the following pattern:

3332	0010	0120	1101	3210	1121	3110	3322
0130	1021	2311	2331	2031	0232	3212	1111
3330	0020	0300	2203	3020	2303	2221	3310
0320	2103	1223	1323	0122	1131	3030	2223

- Message Structures — The structure and content of all signals and messages used for transferring information between FSVS network elements or for controlling the network.

- Media Processing — The supervisory signals, modem scrambling, modulation, and other provisions (e.g., forward error correction coding) necessary to be compatible with the communications network.

The Signaling Plan is organized along the following lines. Chapter 2 specifies the FSVS signaling protocols for Plain Old Telephone Service (POTS), STU-III Terminal-Terminal Interaction and STU-III interaction with the Key Management Center and other network interfaces. Chapter 3 specifies all of the media processing including the modulation, message scrambling, and coding. Chapter 4 catalogs and fully specifies all signaling and supervisory messages. The Signaling Plan concludes with a list of acronyms in the Appendix.

1.2 DEFINITIONS

The following terms are used throughout this document:

- Initiator — The terminal that initiates the secure call set-up. Based on the signaling design, this is the terminal that sends either the 2100 Hz Echo Suppressor Disable (ESD) tone or the 2100 Hz Echo Suppressor/Canceller Disable (ESCD) tone (for full duplex operation) or the P1800 Hz carrier (for half duplex operation) to begin the analog voice to secure voice/data signaling.

- Responder — The terminal that responds to the signaling sequence started by the initiator.

The pattern shown is the first part of both the pattern at SCR_{out} in Figure 3-1 and the pattern that should be transmitted to the distant end during the scrambled ones phase of modem training (i.e., the pattern at D_s). In Figure 3-1, D_i is all zeros for SCR1.

4.1.4 SOM/Start

Start is a 32 dibit long sequence that is used to synchronize the beginning of secure traffic. Start of Message (SOM) is the same dibit pattern. It is used in every transmission to define frame synchronization. Both are transmitted MSB first. Start and SOM are always sent as complete 64-bit (32-dibit) messages and are never truncated.

4.1.4.1 SOM/Start Used by the Initiator

The SOM/Start pattern used by the initiator corresponds to the dibit sequence:

1332 0020 1202 2132 2032 1023 1312 1222

This pattern may be referred to as SOM(C), Start(C), or ST(C).

4.1.4.2 SOM/Start Used by the Responder

The SOM/Start pattern used by the responder is the inverse of the pattern used by the initiator and corresponds to the dibit sequence:

2001 3313 2131 1201 1301 2310 2021 2111

This pattern may be referred to as SOM(A), Start(A), or ST(A).

- Leader — The terminal that begins a signaling sequence as a result of some user/machine determined condition, e.g., out of sync detection, voice/data transition, activating the non-secure control, or an error (failed call) condition.

- Follower — The terminal that responds to the signaling sequence started by the leader.

- Calling Party — The subscriber who dials the initial telephone call.

- Called Party — The subscriber who receives the initial telephone call.

- Local — The terminal where operation is presently being described.

- Remote — The far-end terminal.

- E/P — encrypted/plain — A message structure in which the data is encrypted while the BCH error protection coding is sent in the clear (unencrypted).

1.3 REFERENCED DOCUMENTS

The following documents in effect at the date of this Signaling Plan form a part of this specification to the extent specified in this document. In the event of a conflict, this document shall take precedence on issues related to FSVS signaling.

AT&T Co. Publication 61100, "Description of the Analog Voiceband Interface Between the Bell System Local Exchange Lines and Terminal Equipment," dtd January, 1983.

AT&T Co. Publication 41101, Technical Reference Data Set 103A.

```
Polynomial:  X^-23 + X^-18 + 1
Seed:        01000100010001011100010
             ↑
             First Bit Into Scrambler

Di:  all zeros for SCR1
```

0011001100000010	1011011101011001	0101011101000111	0001100010000000	1
1011011111101110	1101001101101011	1001011010000011	1100110101110010	2
0000101100111001	1001100100100111	1110101010000100	0100101010001011	3
1110010111001000	0001000101000110	0110101110001100	1110100111001011	4
1101110001011110	1001111101010000	1110010100010101	0110011101110000	5
1000110011101101	0011110111011101	0110101011110011	0001111110010110	6
1101111000100101	0110010111001010	1110110001000110	1101000100110110	7
1100011000010000	0010001111110111	1101011101000101	1110010110000000	8
0000110101010100	1111110010110000	0110100100101010	1000010101100111	9
0000101110101100	1111001100000011	1001101011011001	0001111001111100	10
0000101001011100	0000010101111100	0100011010101010	0001011011011000	11
0010111001100100	0100010000111010	0010011001111001	0000001000101101	12
0100110101110000	1111011000111001	0010001110011101	1100010101011111	13
1011010100100010	1010110111011101	0001000111010011	0000000110101000	14
1001100110010110	1000100010101001	0111000011000100	1111000100101111	15
0100101001010110	0111001111111110	1100111111100111	1011000110011001	16
1101110011111010	1011101101111000	1010010001010111	0010011110100010	17
1001100001011000	0001110011011001	0100100011110000	0001111101010010	18
0001100000010101	1101110111001010	1010001100110110	1100001001110100	19
0010001011100110	0001111100000011	1011010000000001	0001010110010111	20
1011100010110001	0011111010100010	1101001000101010	0000111011010001	21
0010100001010110	0001011110111010	1101011000111110	0011111111011100	22
0000110001110111	0100010011111010	1100000001001000	1011101001101101	23
0100000000010000	0111010101111011	1100001001001011	1111100011101001	24
1001011000110100	0100100101011110	1000010100111010	1110001110111011	25
0011001011010110	0100010100101111	1100001000111110	0101000011110100	26
0001011101100011	0001001000001001	1111110101011001	1001001101010011	27
0010100000001101	1001001110101100	1000000000110011	1000011011110011	28
0111100101001110	1100011101011110	1101001110100110	1111011010110001	29
0000111110111110	1101111000001111	0011010111000000	0010110011100100	30
0111010010011111	0010101000110001	0000101100100111	1101111100100000	31
0100011110001001	1010111010010010	1000011100000110	0111101100110000	32

ED87-56

Figure 4-2. GPC Scrambled Ones Pattern (SCR_{out} and D_s)

CCITT Recommendation V.26 bis," 2400/1200 bits per second Modem standardized for use in the General Switched Telephone Network," dtd 1980.

CCITT Recommendation V.32, "A Family of 2-Wire Duplex Modems Operating at Data Signaling Rates of up to 9600 Bits/s for Use on the General Switched Telephone Network and on Leased Telephone-Type Circuits," dtd May 1984.

Defense Communications Agency Circular DCAC-370-V175-6, "System Interface Criteria", dtd September 1978.

Future Secure Voice System Terminal Performance Specification, FSVS-220; Rev. C.

"Principles of Data Communications"; R.W. Lucky, J. Salz, E.J. Weldon, Jr.; Bell Telephone Laboratories, Inc.; McGraw Hill; 1968; page 370.

```
Polynomial:  X-23 + X-5 + 1
Seed:        01000100010001011100010
             ↑
             First Bit Into Scrambler
```

D_i: all zeros for SCR1

1010111011001100	0101100001100001	0110110000101110	0100111101011101	1
0100100100101000	0000010101000111	1001001101101110	0000000011011111	2
1101110100010110	1111011111111010	0000001000000000	0000101110100110	3
1100100110100101	1001111010011000	0111011101111001	0000011100101000	4
0100111110001101	1100000101101011	1011100110110000	1010110111100011	5
1000001010110001	1011010101010000	0001110001110110	1110100010000011	6
0000101001111101	0001000101100000	0000010111110010	1010101010100001	7
0001001000111011	0110011011101100	1110111001000000	0010011100011011	8
1010001010100100	1110111111000100	1001001010110101	1101100000011010	9
0100011001111100	0010101000100010	0001011100010011	0010001011000111	10
1110011010001110	0000000000110011	0111100000111110	0110101001011101	11
0110100001101000	0000010100000111	0001011101001111	1000110110111100	12
1000010011000010	1001001001100101	0101000001011001	1111101010001011	13
0001010010101111	1001010101111101	0100101010000001	0000110100000010	14
1110101010110000	0111100111100101	1011001010011000	1111001100000010	15
1101100011011111	0000001001011100	1010010011011101	1010101111101001	16
0000110011001110	0101111100011110	1001011111111110	0011001101001010	17
0101000100010001	1110010001111110	0010110101011101	1110110011000011	18
0101111011010000	1111111010110111	1110000100001010	1100011000001101	19
1000011001000001	1110101110101110	0000110001001010	1111010001000101	20
0100000000010111	1100101100100110	1110011101010011	0010101101101010	21
0000100111100110	0001101100110101	1001111100110000	0001010001100010	22
1000101110001011	0110000111100111	1101011110000000	0011000111011110	23
0000111111100011	0101100100101001	0111001011011011	0111011010101111	24
0011000010010110	0001000100010110	0110000011011011	0000101101100101	25
0110001011111110	1100001100100011	0001101010101100	1101111100110011	26
0011111110111100	0111101001010010	0001011110110110	1110110010110101	27
0011101111111001	0101111101110011	1001000111001111	0110001111000010	28
0111001010101101	0001001110000110	1001000101010010	0110000111010011	29
1100010100010100	1111111110001001	1001101011010110	0101111000111011	30
1000111100111010	0101101000110000	0000101100010011	0000011111010111	31
0110001011100111	0110101001101001	0111101011111100	1100101101010000	32

ED87-55

Figure 4-1. GPA Scrambled Ones Pattern (SCR_{out} and D_s)

SECTION 2
SIGNALING PROTOCOLS

Secure calls between any Future Secure Voice System (FSVS) terminal equipment, either user terminals or frontend terminals to system components, will employ the same signaling protocol. This uniform Signaling Plan enhances interoperability among different terminal equipment types and terminal equipment supplied by various vendors. A universal Signaling Plan forces both the sponsor and the vendors to provide for expansion and upgrades in the initial design stages. Although more complex than limited-purpose signaling plans, a universal protocol by its very nature matures faster and tends to be used by more applications.

The set of common interoperable protocols for calls between various FSVS network elements is presented in this chapter. The protocols are presented using state transition diagrams for each of the major phases of the call set-up with flow diagrams to document the specific functions and operations required within each state. This is supplemented, where appropriate, with timing diagrams or timelines for the actual message transmissions.

The state transition diagram shown in Figure 2-1 depicts the highest-level states and the basic conditions which cause transitions. This can serve as a roadmap to the call set-up. The call set-up is segmented into six phases, as indicated in Figure 2-1:

- Plain Old Telephone Service
- Initial Call/Modem Training
- Variable Exchange
- Cryptosync/Resync
- Secure Traffic
- Call Interruption Handling

phase reversals and may be interrupted with transmission of a "Message B" as described in the discussion of divergence from the interoperable mode in Section 2.2.1.2. In all of these variations the P1800 message is terminated with the "3202" dibit sequence prior to the transmission of SCR1.

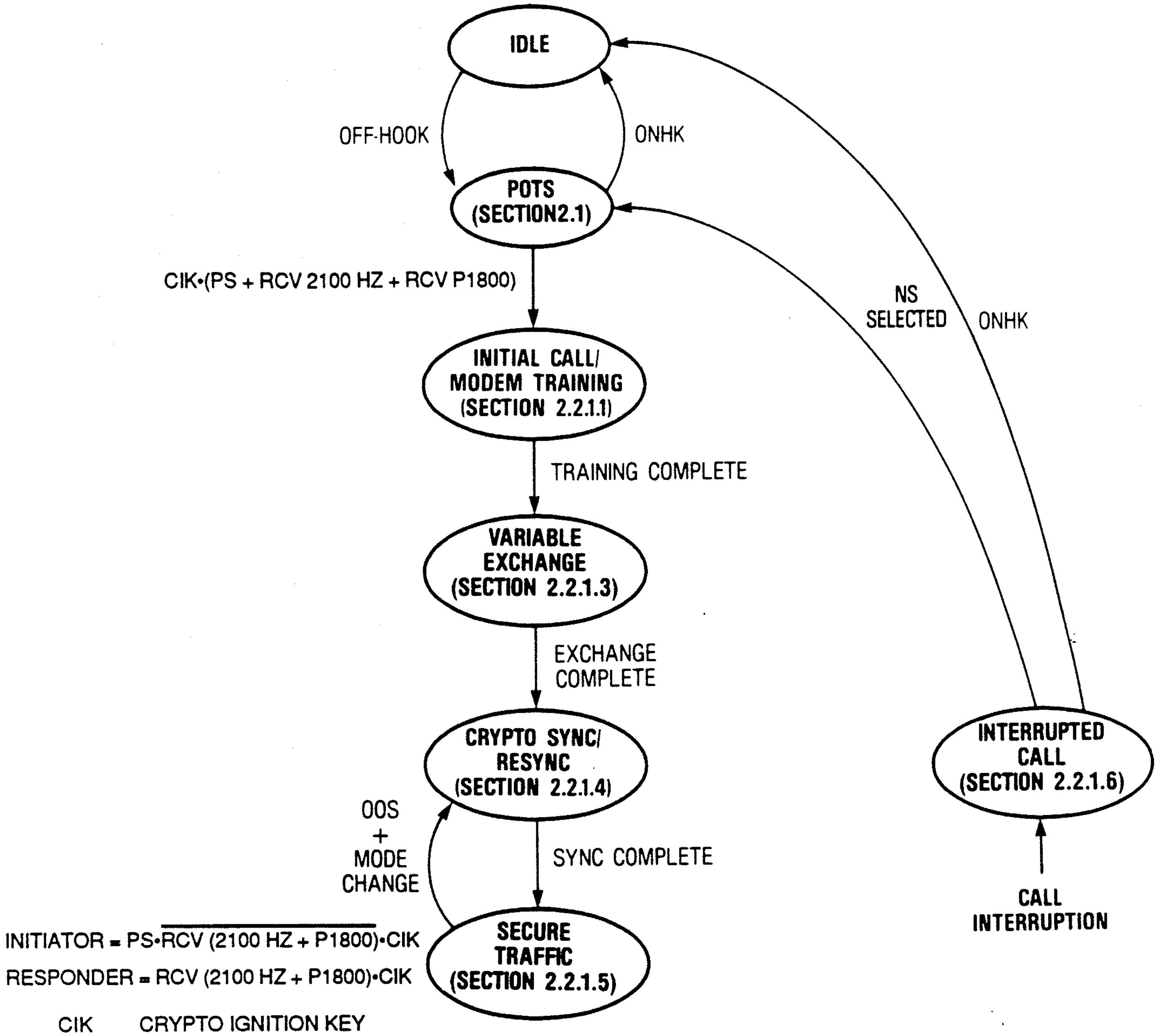
4.1.2 Network Echo Control Tones (ESD/ESCD)

The Echo Suppressor Disable tone, ESD, is a 2100 Hz continuous phase tone that is used to disable echo suppressors in the network. The Echo Suppressor/Canceller Disable tone, ESCD, is a 2100 HZ tone with periodic phase reversals which occur every 450 ± 25 ms. As a minimum 2 phase reversals must be transmitted. The 2100 Hz tone shall be generated with an accuracy of 2100 Hz ± 0.01%.

The STU-IIIs will have an ESD/ESCD "strap" which is used to select one of these signals for use during the first phase of modem training. Wherever "ESD" is used by itself in the text and Signaling Plan diagrams, it should be understood generically as "ESD" or "ESCD" as determined by the setting of the ESD/ESCD strap. Where "ESD/ESCD" is used in the text and diagrams, it should be understood to be either ESD or ESCD as selected by the ESD/ESCD strap.

4.1.3 Scrambled Ones (SCR1)

The scrambled ones sequence (SCR1) is used to allow the acquisition of baud sync and train the modem equalizers. The SCR1 sequence for the initiator shall be the bit pattern generated by the GPC scrambler, seeded as shown in Figure 4-2. The SCR1 sequence for the responder shall be the bit pattern generated by the GPA scrambler, seeded as shown in Figure 4-1. The first part of the SCR1 (GPC) and SCR1 (GPA) are shown in Figures 4-2 and 4-1, respectively.



CIK	CRYPTO IGNITION KEY
NS	NON-SECURE
OFFHK	OFF HOOK
ONHK	ON HOOK
OOS	OUT OF SYNC
PS	PUSH SECURE
RCV	RECEIVE

ED87-102

Figure 2-1. Overview STU-III Terminal Signaling State Transition Diagram

4.1.1.1 Half Duplex Use of P1800

When initiating a half duplex transmission sequence, P1800 shall contain 388 dibits (776 bits) of the dibit sequence "0202". This P1800 sequence shall be followed by the sequence "3202" so that the last dibits transmitted will be ...02023202. This P1800 message is always followed by an SCR1 message as described in Section 2.2.2. Prior to transmitting the P1800 message, the transmitter shall verify that the transmission link has been idle (no carrier present in either direction) for a minimum of 35 ms.

A terminal may initiate a half duplex transmission with fewer than 388 dibits of "0202" in three circumstances: (1) when transmitting half duplex secure voice traffic, (2) when the direction of transmission on the channel is the same as that of the previous transmission, and (3) when the transmitter has verified that the channel has been idle for more than 35 ms, one dibit may be eliminated for each 1/1200th of a second of additional idle time. In each of these cases, the terminal shall transmit at least 188 dibits of "0202" prior to the "3202" sequence and SCR1 described above. This permission to shorten the length of P1800 does not apply, however, to the P1800 transmitted by the initiator prior to CAP/SV during call setup.

4.1.1.2 Half Duplex Initiator's Use of P1800

In half duplex signaling the initiator transmits a segment of P1800 to start secure call setup. In this application, the P1800 message is only 512 dibits long (1024 bits). It is not terminated with the 3202 sequence and is followed by a drop of carrier prior to the transmission of a standard P1800 message to continue call setup.

4.1.1.3 Full Duplex Responder's Use of P1800

In full duplex signaling, P1800 is transmitted in response to the initiator's request to start secure call setup. As described in Section 2.2.1, the length of the P1800 message in this application is determined by the initiator's response to the P1800 message. In addition, this P1800 message may begin with a series of

Each of these phases is discussed within this chapter. The Chapter is divided into four sections. Section 2.1 describes the STU-III operation in providing Plain Old Telephone Service. Section 2.2 addresses the remaining five call set-up phases for full duplex and half duplex operations. Section 2.3 describes the Type I terminal interaction with the Key Management Center as it differs from normal STU-III/STU-III calls. The chapter concludes with Section 2.4 providing a discussion of the STU-III interaction with a network front-end, referred to as a Line Interface Terminal.

2.1 PLAIN OLD TELEPHONE SERVICE (POTS)

The following is a very brief description of the signaling to support POTS. It is based on, and consistent with AT&T Publication 61100.

All calls are established as a plain analog connection through the network employing a common dialing procedure. For public switched telephone network calls, the originator going off hook causes a service request to the network as a DC loop closure. The network detects the service request and returns a dial tone to the originator. The local network switching equipment expects directory number information either as dial pulses (DP) or as Dual Tone Multiple Frequency (DTMF) tones.

The user enters dialing information via a keypad on the user terminal. The terminal generates DTMF tones or outpulses the dialing information on the loop while the keying is in progress.

During the call establishment process, the network will return call progress information such as trunk busy, station busy, ring back, "no such number", etc. to the originator, as analog tones or announcements. The network does not provide answer supervision to the originator who depends on a verbal response when the called party answers the call.

Table 4-1. Message Catalog

Supervisory	Data Bearing
P1800	CS VOICE (FDX)
2100 Hz ESD/ESCD	CS VOICE (HDX)
SCR1 (GPA)	CS FULL RATE DATA (FDX)
SCR1 (GPC)	CS FULL RATE DATA (HDX)
SOM	CS HALF RATE DATA (FDX)
START	CS HALF RATE DATA (HDX)
EOM	CS ONE-WAY VOICE (FDX)
FILLER	CS ONE-WAY FULL RATE DATA (FDX)
ESCAPE	CS ONE-WAY HALF RATE DATA (FDX)
	CS ONE-WAY SECURE DIAL (FDX)
Non-Data Bearing	CS SECURE DIAL (HDX)
	CS BERT (FDX)
RELEASE	CS BERT (HDX)
ABORT	CAP/SV
FAILED CALL	TC
RESTART FAILED CALL	RCC
IDLE	
RETRAIN REQUEST	
RETRAIN ACK	
RETRAIN NACK	
	Message Traffic (Half Rate)
	REKEY
	RK ACK
	CKL
	CKL ACK
	DIAL DATA

On the called side, the network will signal an incoming call via an AC ring signal on the loop. The called party answers the call by going off hook which closes the DC loop. The network, at this time, stops ring on the called line and ring back on the calling line and establishes a plain analog connection between the calling and the called parties.

Either party can terminate the call by going on hook which opens the DC loop to the network. Depending on the switching equipment employed in the network, different disconnect timeouts for calling or called parties are employed. The network will mark it idle. If a terminal remains off hook, it is timed; upon time-out a howler (permanent off hook) is connected for approximately ten seconds after which the loop is locked out. Upon going on hook, the loop is placed in an idle state by the network.

2.2 STU-III TERMINAL-TERMINAL INTERACTION

This section provides the detailed signaling and protocols for establishing a call between two STU-III terminals. Separate descriptions are provided for full duplex and half duplex operation. This section focuses on operation over two-wire commercial telephone networks. An additional section has been allocated to specify a higher rate (4800 bps) mode, however, this will be incorporated into the Signaling Plan in a future version. The section concludes with a discussion of the implications of operation over the AUTOVON/Defense Switched Network and Cellular Radio networks. There is another section allocated for the specification of a Digital Network (56/64) kbps mode which will also be provided in a future version of the Signaling Plan.

The STU-III signaling is designed to provide reliable and responsive secure call operation in several modes and options. Under normal situations, the STU-III shall provide Plain Old Telephone Service (POTS) operation (as described above) as well as allowing the user to initiate a secure call set-up manually. The STU-III also shall provide two "strap" options, normally selected at installation. One strap will be an "Auto-Secure on Receive" strap

SECTION 4
MESSAGE FORMATS

This chapter specifies the messages and the interaction with the network and transfer information between various FSVS component equipments. The messages are divided into three categories:

- Supervisory
- Non-Data-Bearing
- Data-Bearing

Table 4-1 provides a list of the specific signals and messages within each category. The remainder of this chapter specifies the structure, content, and format for each signal. The supervisory and non-data bearing messages are included in this report. The data bearing messages are described in a classified attachment.

4.1 SUPERVISORY MESSAGES

Supervisory messages are used to support the networking signaling, modem operation, and to alert the far end STU-III that a change is about to occur, or to allow for differences in processing times between terminals. P1800, ESD and SCR1 are primarily associated with the initial call or modem training. SOM, Start, Filler, EOM and Escape are primarily sent during traffic. Supervisory messages are not BCH-coded or encrypted in any way. In addition, with the exception of filler, supervisory messages are not scrambled.

4.1.1 Pseudo 1800 Hz (P1800)

The P1800 message (Pseudo 1800 Hz) consists of alternations of the dibits 00 and 10, corresponding to +45 and —45 degree phase shifts, respectively. P1800 is used primarily in half duplex to initiate a half duplex transmission sequence. It is also used, however, in two other places: (1) by the initiator in half duplex to start call setup, and (2) by the responder in full duplex to answer the initiator's request to start call setup.

and the other will be a "Plaintext Inhibit" strap. The terminal will have the capability to have either strap option selected separately, or both simultaneously. When one of these options is selected, the terminal will deviate from otherwise normal operation as described below:

- Auto-Secure on Receive — When the terminal is strapped for this option, it will immediately initiate a secure call set-up when the user goes off hook to answer an incoming call. Beyond that, the terminal will operate normally to place calls, to permit a User Abort (activating a Non-Secure control), Failed Call or other options available to a normally strapped STU-III.

- Transmit Plaintext Inhibit — When the terminal is strapped for this option, it will never be able to transmit speech in the analog clear mode. When placing or receiving calls, the terminal will bridge the handset receiver to the line but the microphone will be muted. The secure call will be initiated by the user activating the Secure control. During the secure call or call set-up, the call may be interrupted as in a normally configured STU-III, however, the microphone is only connected during secure operation. If the Non-Secure control is activated to abort a call, or in response to a Failed Call, the call is interrupted but only the hand-set receiver will be bridged to the line; the microphone will be muted.

- Auto-Secure Transmit and Receive — Transmit plaintext inhibit and auto-secure on receive may be used in combination. If the CIK is not connected, the STU-III will remain in the POTS mode with the microphone disabled.

These straps are intended as installation options and are planned for use in special government applications; a STU-III with this strap(s) selected need not operate completely behind certain PABX configurations. Unless otherwise stated, the remainder of this section will describe operation assuming these options are not selected.

Table 3-2. Factors of g(X) for (255,131) BCH Code

Polynomial	Nonzero Coefficients	Hexadecimal
$m_1(X)$	8,4,3,2,0	11D
$m_3(X)$	8,6,5,4,2,1,0	177
$m_5(X)$	8,7,6,5,4,1,0	1F3
$m_7(X)$	8,6,5,3,0	169
$m_9(X)$	8,7,5,4,3,2,0	1BD
$m_{11}(X)$	8,7,6,5,2,1,0	1E7
$m_{13}(X)$	8,5,3,1,0	12B
$m_{15}(X)$	8,7,6,4,2,1,0	1D7
$m_{17}(X)$	4,1,0	013
$m_{19}(X)$	8,6,5,2,0	165
$m_{21}(X)$	8,7,3,1,0	18B
$m_{23}(X)$	8,6,5,1,0	163
$m_{25}(X)$	8,4,3,1,0	11B
$m_{27}(X)$	8,5,4,3,2,1,0	13F
$m_{29}(X)$	8,7,3,2,0	18D
$m_{31}(X)$	8,5,3,2,0	12D

2.2.1 Full Duplex (2 Wire), 2400 bps Operation

The user goes off hook and dials the called party either directly, or through operator assistance depending on the user's installation. In the normal sequence, one or both users decides to go secure and initiates the secure call set-up. Either user presses the Secure button (or performs a comparable action) and the terminals exchange the appropriate protocols.

The STU-III shall incorporate the timeouts shown in Table 2-1 when waiting for a message from the far-end terminal. In addition, the STU-III shall enter a Failed Call sequence (Section 2.2.1.6.2) if carrier is lost for five seconds or more. The STU-III shall "start" the timer upon transmission of the sequence indicated in Table 2-1, column B, and shall "stop", reset, or disregard the timer upon detection of the expected message sequence response, also indicated in Table 2-1, if the message sequence is detected before the timer value is exceeded.

The STU-III shall not timeout if the expected message sequence is received either before the timer is set, or before the timer value is exceeded.

If the timeout occurs during modem training, the terminal that times out shall stop any signaling and prompt the user to activate a nonsecure control to reenter the analog mode. If the timeout occurs during the variable exchange phase, the terminal that times out shall enter the Failed Call sequence. If the timeout occurs while waiting for a response to a cryptosync, the terminal that times out shall either transmit another cryptosync message or shall enter the Failed Call sequence, depending on the terminal design. The STU-III shall not timeout during a secure traffic mode or during a call interruption sequence that does not lead to a resync. Table 2-1 defines the conditions and results of the specified timeouts for FDX operation.

Once a secure call is initiated, the terminals exchange status, crypto variables and crypto synchronization data with a series of message transfers and then enters secure traffic. The primary mode of the STU-III terminal is 2400 bps and are unaltered since the code is systematic. The switch is then thrown and the 124-bits remaining in the storage elements are clocked out as bits 1-124 of the codeword (where the first bit transmitted is the bit 124 of the codeword). The time order of transmission is thus most significant bit to least significant bit. Finally, a single zero bit is appended as bit 0. Note: The BCH data block may contain padding of up to 127 bits in the event that the data for the final block does not have exactly 128 bits.

The feed back taps are the coefficients of the generator polynomial of the code. The factors of the generator polynomial are listed in Table 3-2 (also available in Principles of Data Communications). The entries in this table list the powers of X which have nonzero coefficients. For example, the notation (8,4,3,2,0) represents the polynomial

$$m_1(X) = X^8+X^4+X^3+X^2+1$$

The table also lists the alternative representations as hexadecimal numbers for X=2. For example, the above polynomial as hexadecimal is $m_1(2) = 11D$.

The complete generator is a 124th degree polynomial:

$$g(X)=m_1(X)*m_3(X)*m_5(X)* \ldots *m_{31}(X)$$

$$= g_{124}X^{124}+g_{123}X^{123}+ \ldots +g_1X^1+g_0$$

where $g_{124}=g_0=1$.

In the hexadecimal form: g(2) = 11BC B6CC E690 6958 AA17 F223 1050 EB39

This code has minimum distance 37 and therefore can correct up to 18 errors in each received block.

Table 2-1. Full Duplex Signaling Timeouts

The appropriate terminal, as indicated in column A, shall set a timer during selected points in the call/call set-up as indicated in B. The timer setting is defined in C. If the timeout is exceeded before the expected message in D is detected, the terminal shall enter the signaling sequence in E.

A	B	C	D	E
Terminal Setting Timer	Message Transmitted, Starts Timer	Timer Value	Expected Message Response	Response to Timeout
Initiator	Start of First 2100 Hz ESD or ECHO SUPPRESSOR DISABLE	3.3 ± .7 sec	P1800	Revert to analog call. Prompt user ESCD to abort call
Responder	Final bit of SCR1 "SCRAMBLED ONES"	2.5 ± .6 sec	2100 Hz	Revert to analog call. Prompt user to abort call
Initiator	Final bit of CAP/SV	3.5 ± .6 sec	SOM of CAP/SV	Failed Call
Either Terminal	Final bit of TC	2.5 ± .6 sec	SOM of TC	Failed Call
Either Terminal	Final bit of RCC	2.5 ± .6 sec	SOM of RCC	Failed Call
Initiator	Final bit of RCC Final bit of initial CS	6.5* ± .6 sec 2.5* ± .6 sec	 SOM of CS	After both timers have expired repeat initial sync, or Failed Call
Initiator	Final bit of retry of initial CS	2.5 ± .6 sec	SOM of CS	Repeat initial sync or Failed Call
Responder	Final bit of RCC	10.0 ± .6 sec	SOM of CS	Failed Call
Either ** Terminal	Final bit of start	2.5 ± .6 sec	Start	Initiate Crypto Resync or Failed Call
Leader	Final bit of CS mode change	2.5 ± .6 sec	ESC sequence (any)	Repeat CS mode change or Failed Call

allowed to Retry 3 times

*A terminal may, alternatively, use a single timeout of 6.5 ± .6 sec after the final bit of the initial CS, if desired.

**This timeout is optional and applies to secure voice mode only.

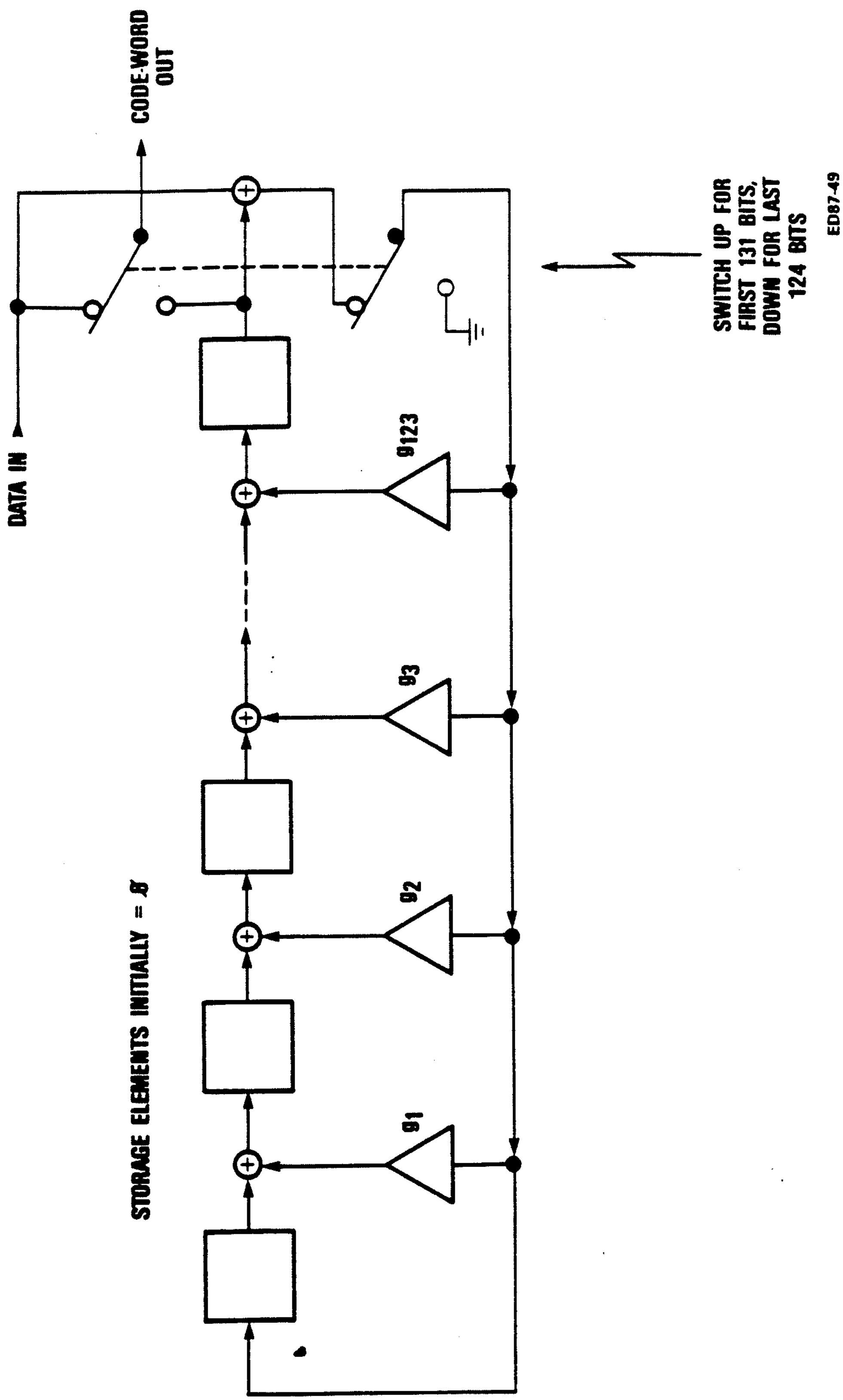


Figure 3-6. BCH Encoder

secure voice. If mode conflicts occur, the STU-III shall default back to secure voice operation. The STU-III may enter the secure data mode initially (without entering secure voice). Once the terminal enters a secure mode, it shall continue processing traffic until the mode is changed, an out-of-sync condition is detected, or the call is interrupted (e.g., by detection of an alarm condition, by the user activating a Non-Secure control, or by the user going on hook).

2.2.1.1 Full Duplex Initial Call/Modem Training

The signaling sequence for this phase of the call set-up is addressed in two segments. The first segment addresses the normal signaling that will be used by two terminals that do not wish to attempt to diverge from the interoperable signaling mode. The second segment addresses the initial provisions needed to support the alternate signaling.

Interoperable Mode Signaling. The initial call/modem training phase of the secure call set-up provides for the network signaling, modem equalizer and modem echo canceller training and baud synchronization. The first terminal to initiate the secure call sequence (i.e., either the terminal whose secure control is activated, or the called terminal if the Auto-Secure option is selected) will assume the role of "initiator"; the other terminal assumes the role of "responder". Figure 2-2 depicts the state transition diagram for this phase and Figure 2-3 depicts the associated timeline. The initiator will send the 2100 Hz Echo Suppressor Disable (ESD) tone or the 2100 Hz Echo Suppressor/Canceller Disable (ESCD) tone depending on the setting of the ESD/ESCD strap. Prior to the generation of this tone, the terminal will first check to ensure it is not receiving a 2100 Hz tone in order to reduce the possibility of creating a glare condition. The responder will detect the tone and wait 1 second before sending the Pseudo 1800 Hz (P1800) carrier modulated by a repetitive 02 dibit pattern. The one second wait shall be observed whether the responder terminal is proceeding as the full duplex responder or the half duplex initiator. The initiator turns off the 2100 Hz tone 90 ms after detecting carrier (P1800 Hz) from

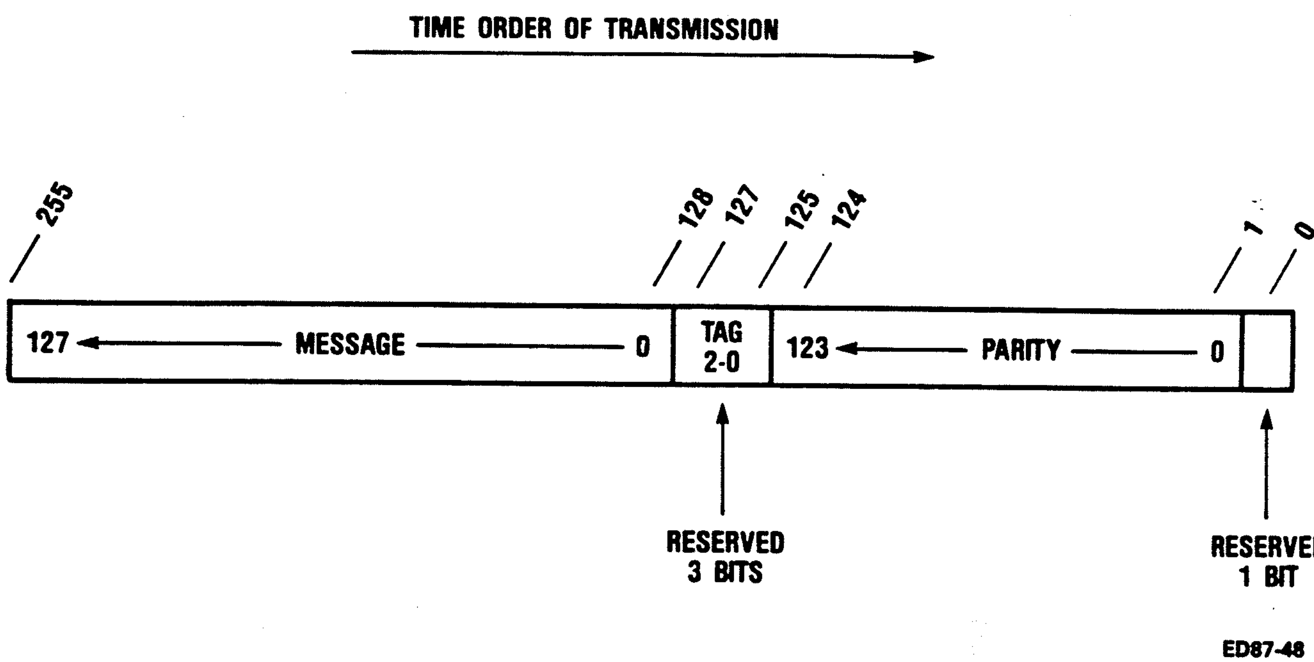


Figure 3-5. BCH Code Block Format

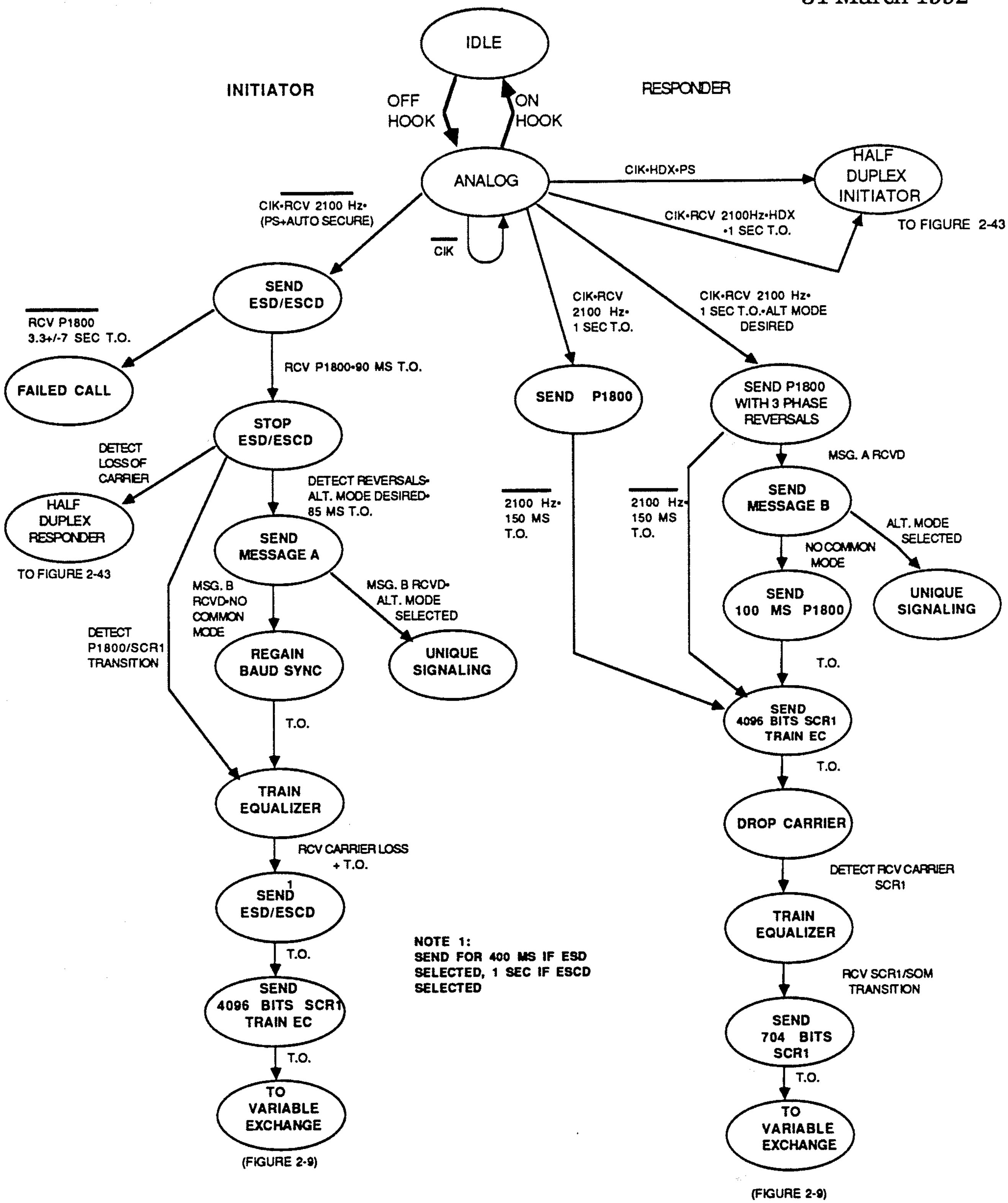


Figure 2-2. Initial Call/Modem Training State Transition Diagram

```
Polynomial:  X^-23 + X^-5 + 1
Seed:        ⇨10010110111011001101010
             └First Bit Into Scrambler
```

D_i: Data to be scrambled

0011100011010101	1000011110110011	1100101010100101	1011010111000100	1
1001000000010100	1101000001011101	0011111110100010	0101011100111001	2
0111000011010111	0011010010111011	1000110111111001	0100001011110011	3
1001000111110101	1011010101110111	1010100111011011	1100111011011010	4
1001110010000110	0111100100001110	1000011100110100	0100000011110110	5
0010011001001100	0111000000110010	1111000010011011	0100000000011110	6
0011100010111010	0001001100010110	0011101000001001	1001111101110000	7
0110111110111100	1111100011100111	1011101111010000	1011010100100001	8
0101010000110100	0001110110111010	0100010111101011	1101010111011010	9
1111111110101001	0000001000010000	0010110010011111	0010011010010010	10
0101001100101011	1000011101100010	1011110100011001	1111010100101100	11
1010100101011111	0101110001001111	0011100010000011	0111101001011100	12
0001100111000101	0110110010101001	0011110011000000	1010100011000000	13
0111110101000100	0101110111101010	0010011001110111	1001011100001011	14
0100101010000101	1100011101010000	0111011111001111	0010011000100001	15
0110101011100100	1001100111100101	0001111000111101	1101101100011011	16
0101111010111100	0010100000000010	1001001100110110	0100100010011101	17
0111100010101011	1001100111000000	1010110110100001	0111010100001100	18
1101101111001011	1011101110010100	1100111011111111	0010111100011010	19
1101011100011001	0000001001000011	1101001101100000	0111101110000101	20
0001011110110101	0101111100101001	1101101110011101	0100011001111011	21
0001110110011111	1111011001110111	0111101111001101	0111101011011110	22
1001000110000110	0111000101010110	0100000100010101	1111110010011001	23
0001110011100001	1100001111011000	1111101110100101	0110010100100001	24
1011100011110010	0010110111100001	0001001100111101	1101001101000011	25
1001100010011101	1001010001101101	1010100110011011	1111101101110111	26
0111001110010101	1011110011111111	0010110111101001	0100101111111011	27
1111001011111111	1111011110100111	0011100111011110	0100001110010000	28
1100010101010010	0100110000010101	1111010011000001	1101101011000000	29
0111111110110111	1100000100001000	1101011011001011	1011001111001100	30
0000100011011110	1001001101110101	1110110110110100	1011000110101001	31
1101100001011110	0101111010111010	1001011111111101	0110000111011110	32

ED87-58

Figure 3-4. GPA Message Scrambling Pattern (SCR_{out})

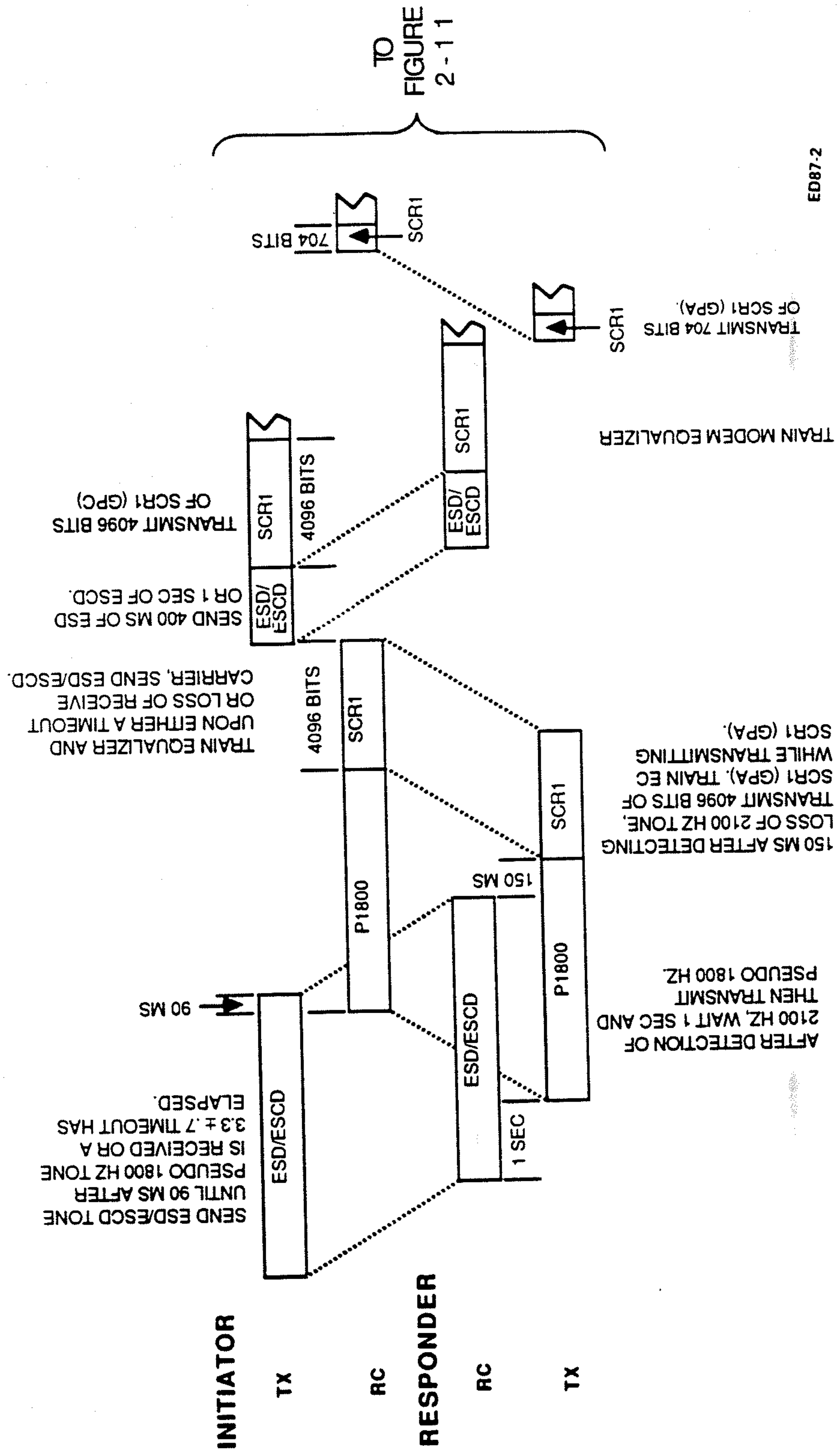


Figure 2-3. Full Duplex Modem Training Signaling Diagram Responder Not Interested in Alternate Mode (Default 2400 bps Interoperable Mode)

```
Polynomial:  X^-23 + X^-18 + 1
Seed:        10010110111011001101010
             ↑
             First Bit Into Scrambler

Di:  Data to be scrambled
```

1011010010001001	1000011110110100	1000110100011101	1011010110100010	1
1010100111111100	0001000011010011	0000001111101010	1001100100000010	2
1000110010001101	0101100111000101	1011001100111101	0001100001010110	3
1100001111011010	1110001010001110	1111001010011001	0101111010111100	4
1001101011101101	1010000001110001	0100110010100011	0100111001001110	5
0110101011110000	1111100110010110	0010000001101001	0101101110100101	6
0111101110100001	1110101111100000	1100011011010000	0000111111000110	7
0101110000010001	1110010001000011	1010010100100111	1001000111111100	8
0101010010100011	0001001001111110	0111110101000100	1001110001010100	9
0101000111010010	0100001100101000	1100101110110011	1001110010000100	10
0111111111100111	1110100011111001	1100101000010000	0111111011101111	11
1100000010111001	1101000001010000	1111100001001011	0110000000011101	12
1011000100111000	1010100011010011	1010010010011010	1011000110010000	13
0110011011111000	1100011010001100	0011111111010001	1110100001110100	14
0010011000110010	0001111000111111	0001110001001100	0100011011010100	15
0111011011000111	0100101010100011	1010001111000010	0101000001001000	16
1110111101001101	0101010111110010	0011000000101000	1001011110010101	17
1000101100110101	1011011000100100	1111100100011010	1000100001001011	18
0110100011111101	1011001100010001	0110100001011101	1000011100111000	19
0010010100111111	1000011011111010	0110000101001100	1001001101101110	20
0100001000000010	1011001111111011	0101011001100110	1101110011001010	21
1000010101110100	1100101110101000	0010010010000010	1010011010010110	22
0101001100010111	0100011110011100	0000000010010111	1100011111011011	23
0010000110000110	1000000111011101	0101001010001011	0001000111111000	24
0010110110100010	0000010011001100	0011101011000101	0110100100111011	25
0010111101100011	0100001001111001	1110100111100101	0111011001010101	26
0110100010000110	0000111100001111	0111000000100010	0011110100010111	27
0011010011000000	0001110010100110	0111100011101111	0010110100110101	28
1110101011101000	1110111010010000	0001010110000110	1101101010110101	29
0100010011100111	1100010001001111	1100000101100100	1001000000100100	30
0001001011010110	1011001101101111	1111111001000010	1101111110010011	31
1100110110100100	0010101100001101	1011110101101010	1000101111011111	32

ED87-57

Figure 3-3. GPC Message Scrambling Pattern (SCR_{out})

the responder. If the initiator does not receive P1800 from the responder within 3.3 ± .7 seconds, the initiator shall prompt the user to activate the non-secure control and revert to the analog mode. The responder, upon detecting loss of 2100 Hz, waits 150 ms, transmits the 3202 transition dibit pattern, sends 4096 bits of SCR1 (GPA scrambler) to train its modem echo canceller and then drops the carrier. The initiator detects SCR1 (or change from P1800) and trains its modem equalizer. The initiator, either by detecting loss of carrier or a 1.7 seconds timeout, sends 400 ms of the ESD tone (or 1 second of the ESCD tone if the ESD/ESCD strap is in the ESCD position) followed by 4096 bits of SCR1 (GPC scrambler) to train its modem echo canceller. Immediately following the completion of the SCR1 sequence, the initiator shall transmit SOM and CAP/SV and proceed with the remainder of the signaling for variable exchange. The responder shall detect the receive carrier and SCR1, and train its modem equalizer. The responder shall wait for the arrival of the initiator's SCR1/SOM transition before beginning transmission of the remainder of the full duplex signaling sequence. Within 300 milliseconds after the arrival of the SCR1/SOM transition, the responder shall begin the transmission of 704 bits of the SCR1 sequence (GPA scrambler). This time window is specifically intended to allow, but not require, the responder to delay the beginning of SCR1 until after the reception of the initiator's CAP/SV. Immediately following the transmission of the 704 bits of SCR1, the responder shall transmit SOM and CAP/SV and shall proceed with the remainder of the full duplex signaling. The responder shall transmit CAP/SV to the initiator unconditionally, irrespective of the contents or transmission errors in the received CAP/SV. This next phase of signaling consists of the full duplex variable exchange messages required for secure communications.

Interoperable Mode Signaling Divergence. The following discussion defines the changes to the Initial Call/Modem Training phase signaling (described above) which will permit an option for a STU-III terminal to diverge from the interoperable sequence before modem training begins. Provisions have been included to ensure that the transition is only possible if both terminals involved in the particular call participate in the discretionary alternative, (i.e., front-

The initial part of the bit sequence generated by the GPA and GPC scramblers is presented in Figures 3-3 and 3-4, repsectively. The scrambler is not self synchronizing, but uses a seed so that the far end and near end scramblers start at the same point on their cycles; the scrambler is seeded at the end of each SOM. The information to be scrambled (at D_i) is mod-2 added to the output of the scrambler (SCR_{out}), i.e., the first bit of the scrambler sequence (left upper corner of the figures) is mod-2 added to the MSB of the MID.

The seed pattern for the message scrambling sequence, from the Status Vector until traffic, is the same for the GPC and GPA scramblers, as shown in Figures 3-3 and 3-4, respectively.

In order to accommodate implementations that use a table-look-up message scrambler, the scrambling pattern generated by the scramblers shall be repeated after the first 8192 bits.

3.3 MESSAGE CODING

All data and non-data bearing messages will be protected with a systematic (255,131) BCH error correcting code. This BCH code is also used for half-rate traffic (e.g. rekey traffic, 1200 bps half-rate asynchronous data). The structure of the BCH blocks depicted in Figure 3-5 will be as follows (bits numbered according to their significance, 0 through 255):

Bits 255-128	Data
Bits 127-125	Reserved (presently set to zero)
Bits 124-1	Parity on bits 255-125
Bits 0	Reserved (presently set to zero)

The codewords shall be constructed by a procedure equivalent to the logic shown in Figure 3-6. The message data bits, with three tag bits appended, are clocked into the circuit as shown. (Initially, the storage elements of the circuit are set to 0.) These first 131 bits form bits 255-125 of the transmitted codeword, end), signaling sequence. If either terminal does not participate in the discretionary alternative front-end signaling, the call will continue in the interoperable mode.

The remainder of this section describes the signaling to coordinate the transition from the interoperable mode. Section 2.2.1.2 addresses the alternative front-end signaling protocol that the STU-IIIs will use once both terminals have indicated the desire to transition from the interoperable mode.

A responder terminal attempting to diverge from the interoperable signaling sequence will insert three 180° phase reversals in the P1800 Hz tone. These phase reversals will occur at dibit positions 32, 64, and 96 after the initiation of the P1800 signal. The 180° phase reversals are created by the substitution of a dibit with a value 1 for a dibit with value 2 in the P1800 dibit sequence. For example, the dibit sequence:

0 2 0 2 0 1 0 2 0 2

results in a 180° phase reversal when the modem carrier is modulated by the "01" dibit pair. For simplicity, the phase reversal is defined as occurring where the dibit with value "1" is inserted in the sequence.

An initiator attempting to diverge from the interoperable signaling sequence must examine the first portion (e.g., 80 ms) of the P1800 received from the responder in order to detect the phase reversals. If at least two of the three phase reversals are detected, the initiator shall recognize the request.

In order for the initiator to be able to distinguish between the last phase reversal in the mode change request sequence and the phase reversal at the beginning of SCR1, the minimum duration of the P1800 signal must be 150 ms (for all STU-III terminals). This will prevent any difficulty in resolving the potential ambiguity on connections with minimal propagation delays. The initiator delays the removal of the ESD/ESCD signal for 90 ms after detecting P1800 or as a design option, the initiator may remove ESD/ESCD after detecting

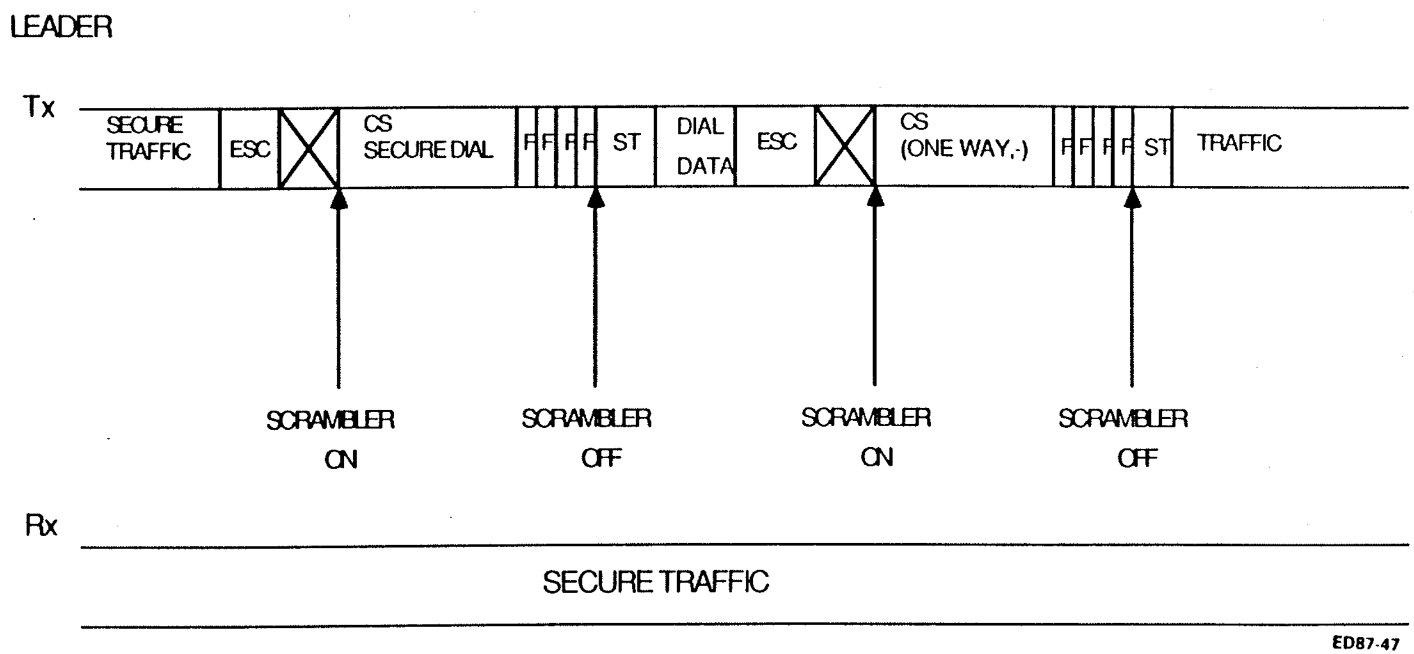


Figure 3-2. Scrambler Usage on Secure Dial Sequence

two phase reversals of P1800. This allows use of a simpler detector for the three phase reversals than would be required if the ESD/ESCD signal were removed immediately upon detection of P1800.

If the initiator determines that an alternative mode is being requested, and is also capable of and interested in diverging from the interoperable mode, it will send the first message of the alternative front-end signaling protocol. Section 2.2.1.2 specifies the maximum time which the initiator may take before detecting the phase reversals and front-end message, and enter the front-end protocol.

A responder not interested in this alternative signaling will simply not transmit the phase reversals within the P1800 signal. An initiator not interested in deviating from the interoperable sequence will ignore the phase reversals in the P1800 Hz. Since these phase reversals occur in the first 80 ms of the P1800, the worst case (zero propagation delay) interval of P1800 received without major phase reversals is 70 ms. This is considered adequate for the initiator to achieve baud sync.

An initiator planning on triggering receiver equalization with the phase reversal at the beginning of the SCRls must take care to avoid premature equalization upon receipt of a mode change request signaling sequence.

2.2.1.2 Full Duplex Alternative Mode Signaling (Option)

This section addresses the alternative front-end signaling required between two STU-III terminals which desire to diverge from the interoperable mode. Section 2.2.1.1 addresses the signaling protocol which establishes the desire of both terminals to diverge from the 2400 bps interoperable mode.

If the initiator determines that the responder has requested an alternate mode, and is also interested in diverging to an alternate mode, the initiator shall send message A, as defined below. If the initiator is not interested, it will await the

Table 3-1. Scrambler Usage

Bit Sequence	Scrambled/	Not Scrambled
SUPERVISORY MESSAGES		
SCR1[1]		X
P1800		X
2100 HZ ESD/ESCD		X
SOM		X
START		X
EOM		X
FILLER	X	
ESCAPE		X
NON-DATA BEARING MESSAGES[2]		
Release (entire 256-bit BCH-coded block)	X	
Abort (entire 256-bit BCH-coded block)	X	
Failed Call (entire 256-bit BCH-coded block)	X	
Idle (entire 256-bit BCH-coded block)	X	
Retrain Request	X	
Retrain NACK	X	
Retrain ACK	X	
DATA BEARING MESSAGES[2]		
All CS messages (entire 256-bit BCH coded block)	X	
CAP/SV (all 256-bit BCH-coded blocks)	X	
TC (all 256-bit BCH-coded blocks, including block containing MID)	X	
RCC (all 256-bit BCH-coded blocks, including block containing MID)	X	
HALF-RATE MESSAGE TRAFFIC		
RK ACK (entire 256-bit BCH-coded block)[2]		X
CKL ACK (entire 256-bit BCH-coded block)[2]		X
Dial Data (all 256-bit BCH-coded blocks)		X
Rekey messages (all 256-bit BCH-coded blocks)[2]		X
CKL Message (all 256-bit BCH-coded blocks)[2]		X
HALF/FULL RATE TRAFFIC		
Secure voice traffic		X
Secure data traffic (full rate or half rate BCH-coded)		X
Secure Bert traffic		X

Note 1: SCR1 is scrambled "1"s, thus the message SCR1 is not scrambled prior to transmission.

Note 2: The 16 bit MID is included in the first BCH-coded block.

150 ms timeout of P1800 from the responder, and then proceed with interoperable signaling. If the responder does not receive message A, it shall proceed with interoperable signaling after the 150 ms timeout of P1800.

Figure 2-3 shows a timeline for the signaling when the responder is not interested in an alternate mode. Figure 2-4 shows a timeline for the signaling when a responder inserts the phase reversals in P1800, but the initiator is not interested. Figure 2-5 shows a timeline for the signaling when the result of the message exchange is that the 2400 bps interoperable mode is used. As shown, the responder shall follow message B with 100 ms of P1800, followed by the 3202 transition dibit pattern prior to sending SCR1. This will allow the initiator to detect carrier and regain baud sync in order to continue with interoperability signaling. Figure 2-6 shows a timeline for the signaling when an alternate mode is selected.

2.2.1.2.1 Message Format The alternative front-end signaling consists of a message exchange between the initiator and the responder. Message A is sent by the initiator to the responder beginning 85 ± 10 ms after removal of the ESD/ESCD signal. Message A conveys a set of desired modes from the initiator. The responder shall examine message A and determine which mode of operation to use. The responder shall format message B with a 1 in the bit corresponding to the selected mode and a 0 in each of the other information bits. The responder shall continue to send P1800 until it is ready to transmit message B. Message B shall be sent by the responder immediately after the end of the P1800 signal. Messages A and B each consist of one or more eight-bit bytes. The first byte of messages A and B shall have the following format where B7 is the first bit transmitted:

B7	B6	B5	B4	B3	B2	B1	B0
1	1	0	X	X	X	X	E

B7-B5: Synchronization bits
B4-B1: Information bits
B0: 1 denotes that an additional byte is required

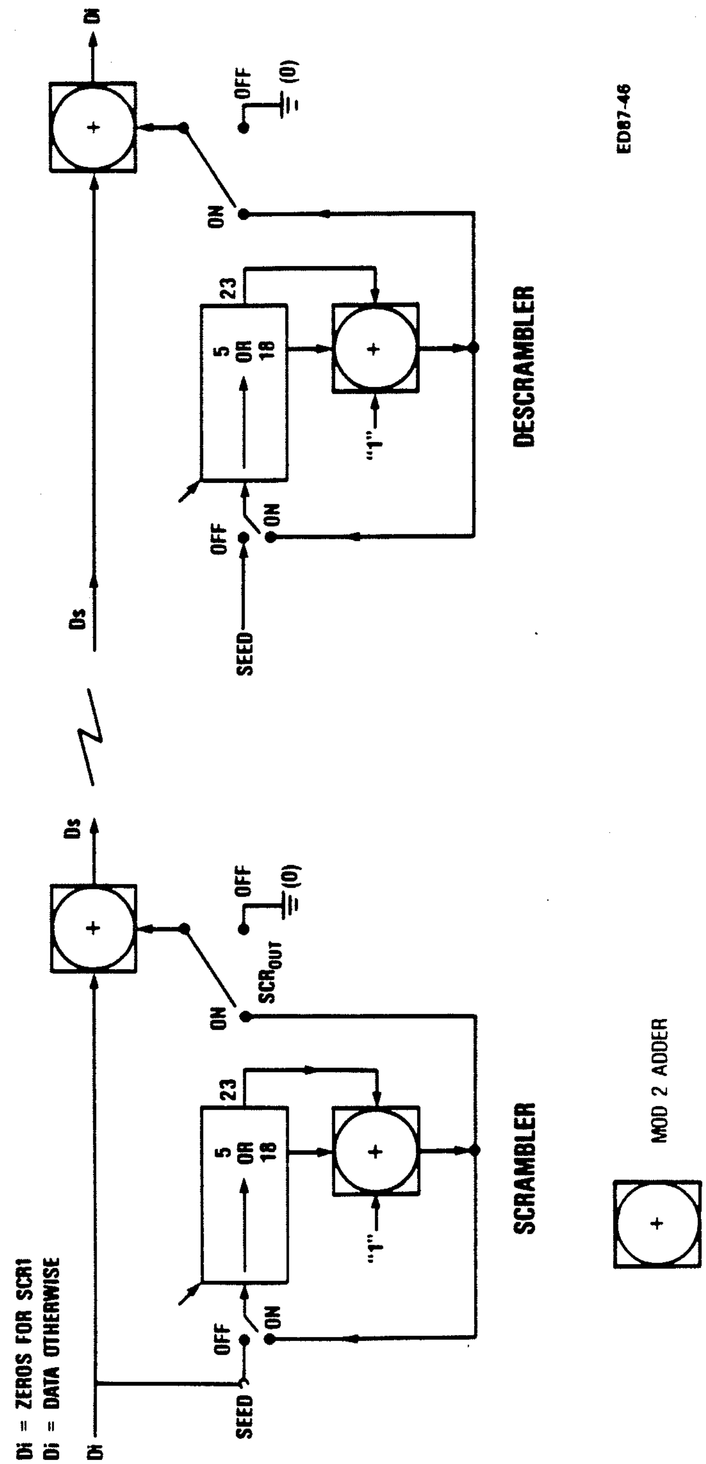


Figure 3-1. Non Self-Synchronizing Scrambler/Descrambler

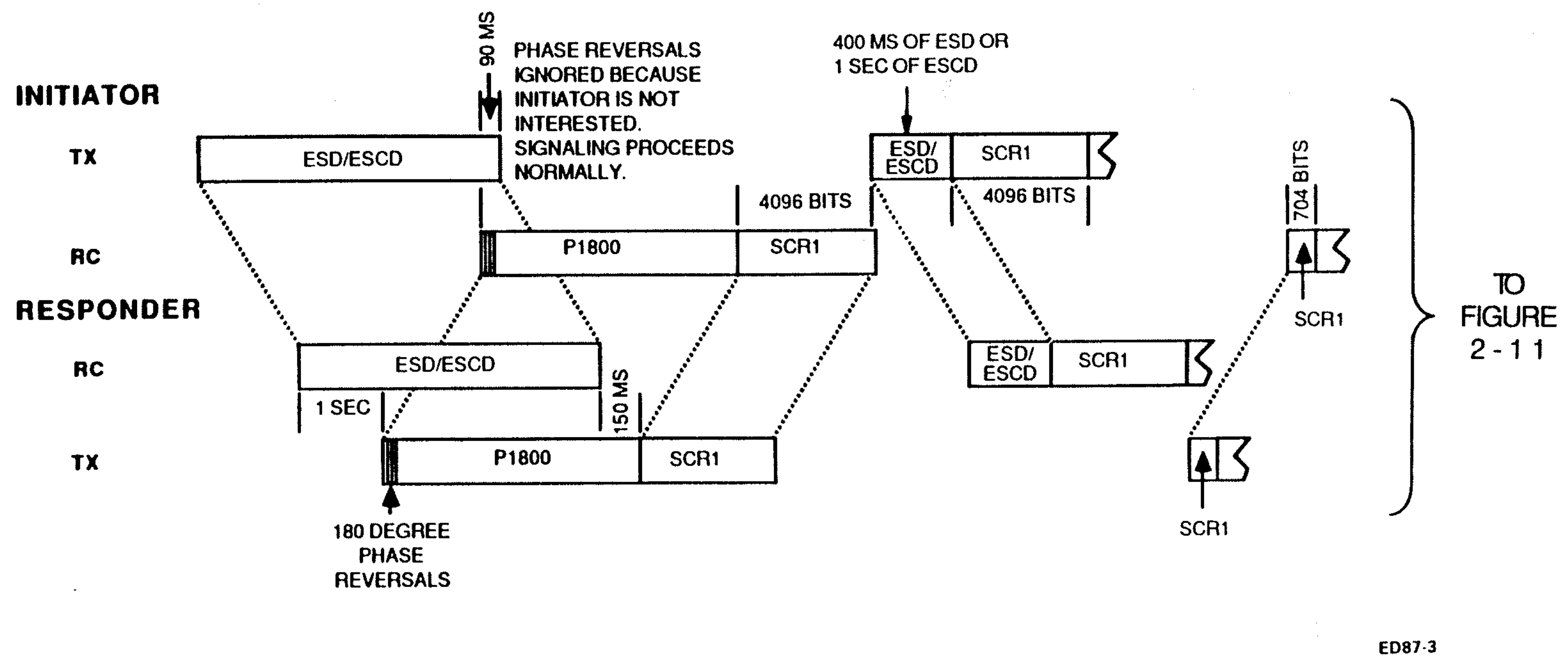


Figure 2-4. Full Duplex Modem Training Signaling Diagram Initiator Not Interested in Alternate Mode

The most significant (left) bit is the first bit to occur in the data stream at the modulator. The demodulator decodes the bits and reassembles them in the correct order.

The terminal maintains baud synchronization so that the first bit of a frame always corresponds to the first bit of a baud.

3.1.2 4.8 Kbps

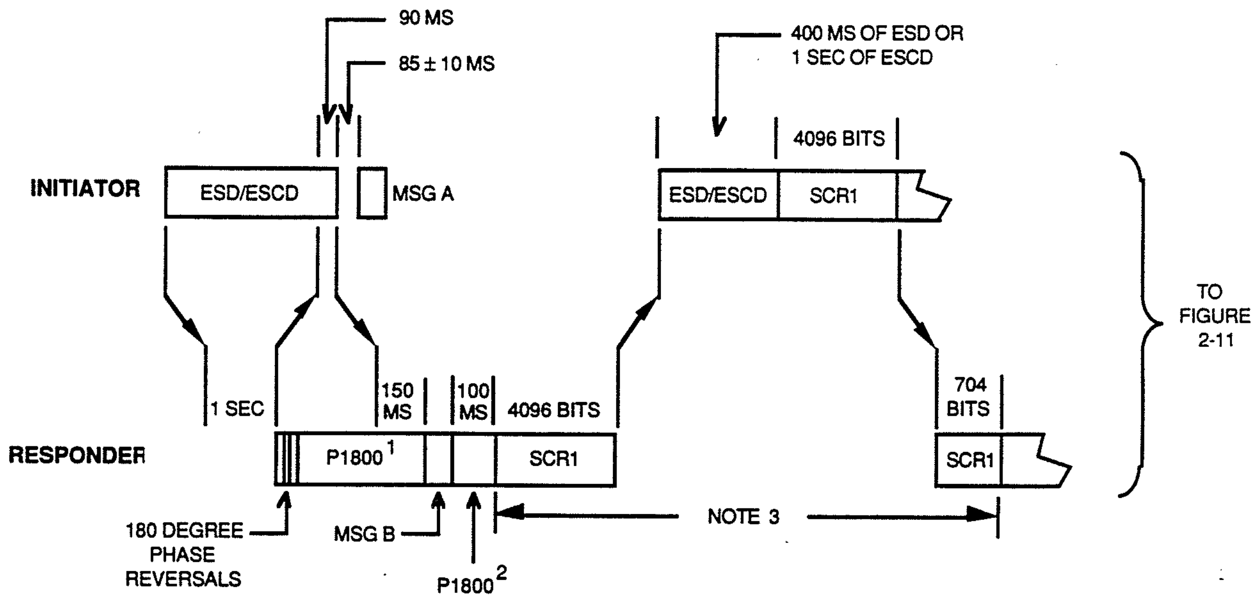
(To Be Supplied Later)

3.2 MESSAGE SCRAMBLING

The scramblers shown in Figure 3-1 are used to scramble the BCH-coded data bearing and non-data bearing messages as indicated in Table 3-1 and described in Sections 4.2 and 4.3 of this document. (Note: The SCR1 message is defined in Chapter 4 and is not considered to be scrambled.) The STU-III shall turn on the scrambler for the first bit of the first BCH-coded block of any of the data bearing and non-data bearing messages. Filler blocks transmitted after a data bearing or non-data bearing message shall be treated as an extension of the message and scrambled with a continuation of the scrambling sequence. The scrambler shall be turned off on the last bit of the message or filler, whichever occurs last.

Supervisory messages, message traffic and traffic enciphered using the traffic key generator are not scrambled. Table 3-1 indicates the STU-III scrambler usage for all messages and traffic. Figure 3-2 depicts the scrambling process for secure dialing.

The initiator of the secure call uses the GPC scrambler, when required, throughout the secure call. The responder of the secure call uses the GPA scrambler, when required, throughout the secure call.



Notes:

1. The responder shall continue to transmit P1800 until MSG A is fully received and MSG B is ready. Message B transmission shall begin within 1 second after carrier drop is detected at the completion of MSG A.

2. If the result of MSG A/B exchange is 2400 bps interoperable mode, after MSG B transmit 100 ms of P1800 followed by 3202 dibit sequence.

3. Same as Figure 2-3.

Figure 2-5. Full Duplex Modem Training Signaling Diagram Interoperable 2400 bps Mode Selected

SECTION 3
MEDIA PROCESSING

The STU-III will provide interoperable operation in two modes: full duplex and half duplex. This chapter defines the modulation, modem scrambling, and coding provisions for these modes.

3.1 MODULATION

The STU-III will incorporate a common modulation scheme to support the two interoperable modes as defined below. This scheme is dibit-oriented. While the message structures defined in Chapter 4 are presented at the bit level for clarity, the modem-to-modem transfers are always transmitted in dibits.

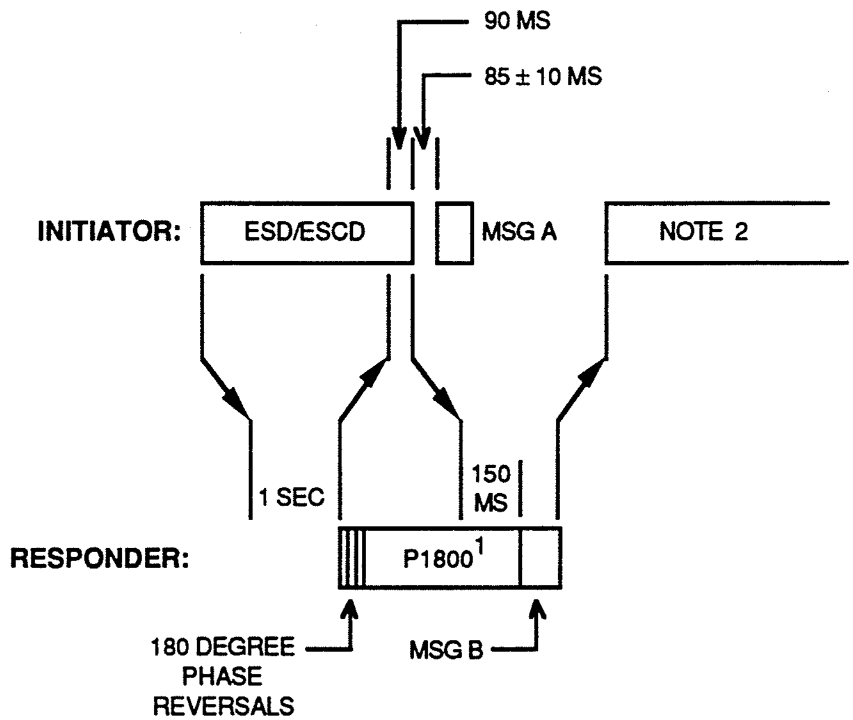
3.1.1 2.4 Kbps

In both full and half duplex modes, the STU-III shall implement the modulation scheme compatible with CCITT V.26 bis as defined below.

The data rate is 2400 +/- 0.24 bps. The baud rate is 1200 +/- 0.12 baud. The transmit carrier frequency is 1800 +/- 1 Hz.

The data stream is modulated by consecutive bit pairs (dibits). Each dibit is encoded as a phase change of the 1800 Hz carrier relative to the phase of the carrier at the end of the previous baud. The phase changes corresponding to the dibits are tabulated below:

DIBIT	PHASE DIFFERENCE (in degrees)
00	$+45^{\circ}$
01	$+135^{\circ}$
11	$+225^{\circ}$ (-135°)
10	$+315^{\circ}$ (-45°)



Notes:

1. The responder shall continue to transmit P1800 until MSG A is fully received and MSG B is ready. Message B transmission shall begin within 1 second after carrier drop is detected at the completion of MSG A.

2. Unique signaling may begin after MSG B.

Figure 2-6. Full Duplex Alternate Mode Signaling Diagram
Alternate Mode Selected

Each succeeding byte in either message A or B shall have the following format where B7 is the first bit transmitted:

B7	B6	B5	B4	B3	B2	B1	B0
X	X	X	X	X	X	X	E

B7-B1: Information bits
B0: 1 denotes that an additional byte is required

2.2.1.2.2 Message Content The contents of the first byte of messages A and B are assigned as follows:

B7-B5: Synchronization bits
B4: 1 for 2400 bps interoperable mode, 0 otherwise
B3: 1 for 4800 bps operation, AT&T Reserved Mode, 0 otherwise
B2: 1 for 2400 bps mode with echo ranging, 0 otherwise
B1: 1 for Motorola Reserved Mode, 0 otherwise
B0: 1 if additional byte in message, 0 otherwise

When the initiator offers alternate modes of operation through the transmission of message A, it shall always offer at least the 2400 bps interoperable mode by setting Bit B4 in the first byte. Other modes offered are at the discretion of the initiator. If no modes are offered from the second and third bytes, the initiator shall terminate message A at the end of the first byte with bit B0 set to "0".

When the responder selects a mode of operation from this first byte, it shall respond with a single bit set to indicate the selected mode and all other bits B0 to B4 set to 0 (including B0 which indicates that this is the last byte).

The second byte is used by STU-IIIs which have implemented the Rec.V.32 modem using the standard V.32 modem training rules. The bits assigned in the second byte are:

If the STU-III line is busy or there is no answer (ten rings), the Gateway operator verbally informs the STU-II user and the connection is terminated.

When the STU-III user goes off hook, the Gateway attendant will inform the STU-III user that a secure call is coming. If the STU-III is unable to receive the secure call (called party not in or CIK not available), the Gateway attendant will verbally notify the STU-II that the call cannot be completed and the connection is terminated. If the STU-III is able to complete the call, the Gateway operator will notify the STU-II verbally that the STU-III is going secure. There will then be a ten second delay, and the user should hold the line.

Once the secure connection from the Gateway to the STU-III has been established, the Gateway attendant tells the STU-II the classification level of the STU-III. At this point, the STU-II has the option of terminating the call if the security level is inappropriate. If the call is accepted at both ends (STU-II and STU-III), then the Gateway operator performs the cut-through as described above.

B7:	1 for 4800 bps operation in the secure data mode using V.32 standard modem training and modulation rules, 0 otherwise
B6:	1 for 4800 bps operation in the secure voice mode using V.32 standard modem training and modulation rules, 0 otherwise
B5:	1 for 9600 bps operation in the secure data mode using V.32 standard modem training and modulation rules, 0 otherwise
B4-B1:	Transmit zeroes (Not available for assignment)
B0:	1 if additional byte in message, 0 otherwise

When the initiator wishes to offer standard V.32 modes for operation, it shall send Message A with the second byte indicating the V.32 modes which it is offering. If no modes are offered from the third byte, the initiator shall terminate message A at the end of the second byte. In this case bit B0 in the second byte shall be set to "0" to indicate that the third byte is not being transmitted. Bit B0 in the first byte shall be set to "1" to indicate that the second byte is being transmitted.

If the responder selects a mode of operation from those offered in the second byte, it shall respond with the single mode bit set indicating the mode of operation selected and all other bits in the second byte set to "0". This includes bit B0 indicating that the second byte is the last to be transmitted. In this case bits B1, B2, B3, and B4 in the first byte shall be set to zero, while bit B0 in the first byte shall be set to 1 to indicate that the second byte is being transmitted.

The third byte is used by STU-IIIs which have implemented the Rec. V.32 modem using the modified V.32 modem training rules described later and by STU-IIIs which have implemented the Motorola proprietary modes for simultaneous voice/data or 9600 bps voice. Both of the Motorola proprietary modes use the modified rules for V.32 modem training. The modes specified by bits B3, B6, and B7 are identical to the comparable modes otherwise specified in the second byte, except that the modes offered in the third byte use the modified rules for V.32 modem training. The bits assigned in the third byte are:

The Gateway then initiates a secure call to the called party STU-II. If the called party's line is busy, the Gateway operator will send the STU-III user a verbal notification of that fact. At this point, the connection to the STU-III will be terminated. Similarly, if the called party is not answering (ten rings), a verbal notification will be sent to the STU-III. The connection will then be terminated.

If the far end terminal (STU-II) is answered and the call setup procedures have established a secure call, the Gateway will then "talk" to the STU-II. The call setup procedure here will be the standard STU-II call setup. The called party will be verbally told that there is a call from a STU-III. The STU-II user will be advised of the STU-III user ID and the classification of the call verbally. If the STU-II user rejects the call, the STU-III user is notified and the connection is terminated.

If the call is accepted, the Gateway operator creates a virtual connection between the STU-II and the STU-III LIT. This "cut-through" will take the operator out of the circuit. Any attempt from the operator to reenter the circuit will terminate the call. The users, however, can get back to the operator via the secure dialing mode (i.e., by dialing Operator, digit 0). Note: All data from the LIT to and from the STU-II's Interface terminal is RED. The Gateway is able to check the status of the call by monitoring the Gateway's communications switch so that billing information can be maintained.

<u>Far End Terminal Calling STU-III</u>. The signaling for a STU-II user calling a STU-III user via the Gateway is similar. The STU-II user first establishes a secure call to the Gateway STU-II front end terminal. If the Gateway answers the call, the Gateway operator verbally requests the STU-II calling party for the called number. This number is assumed to be only for a STU-III connection (i.e., STU-II to STU-II calls are not considered here). At this point, the Gateway operator places the call to the STU-III.

B7:	1 for 4800 bps operation in the secure data mode using modified V.32 modem training rules, 0 otherwise
B6:	1 for 4800 bps operation in the secure voice mode using modified V.32 modem training rules, 0 otherwise
B5:	1 for 4800 bps operation in the simultaneous voice/data mode using Motorola proprietary voice/data bit interleaving rules and modified V.32 modem training rules, 0 otherwise
B4:	Transmit zero (Not available for assignment)
B3:	1 for 9600 bps operation in the secure data mode using modified V.32 modem training rules, 0 otherwise
B2:	1 for 9600 bps operation in the secure voice mode using a Motorola proprietary voice algorithm and modified V.32 modem training rules, 0 otherwise
B1:	Transmit zero (not available for assignment)
B0:	0 (indicates last byte in message)

When the initiator wishes to offer modes of operation from the third byte, it shall send Message A with the first, second, and third bytes indicating the modes which it is offering. Bit B0 in the first and second bytes shall be set to "1" to indicate that the second and third bytes are being transmitted.

If the responder selects a mode of operation from those offered in the third byte, it shall respond with the single mode bit set indicating the mode of operation selected and all other bits in the third byte set to "0". This includes bit B0 indicating that the third byte is the last to be transmitted. In this case bits B1, B2, B3, and B4 in the first byte and bits B1, B2, B3, B4, B5, B6, and B7 in the second byte shall be set to zero, while bit B0 in both the first and second bytes shall be set to 1 to indicate that the second and third bytes are being transmitted.

In offering modes from the second and third bytes, the initiator shall offer modes corresponding to the user's selection from the STU-III control panel or this end, the FSVS program has adopted the concept of providing an FSVS Line Interface Terminal (LIT), which is compatible with the STU-III functions and signaling protocols to serve as a front-end equipment for these network elements.

2.4.1 General Considerations

The STU-III signaling requirements to support operation with an LIT have been structured to minimize the impact to the STU-III design by utilizing the features and signaling inherent in a normal STU-III/STU-III sequence. Features such as secure dialing and data transmission, critical for interfacing to some of these network elements, have been incorporated into the overall STU-III terminal requirements (and can thus be offered between STU-IIIs as appropriate). As it is presently envisioned, the user will merely dial up a network element front-end terminal and establish a secure link as he would with any other STU-III subscriber. The LIT may offer additional interfaces to the network element, however, the intent is for the STU-III basically to operate as it normally does for any secure call.

2.4.2 Manual Gateway Communications

Since the manual Gateway to the BELLFIELD family equipment is a near-term implementation, this section briefly describes the planned STU-III/Gateway operation. There are various steps in a call from a STU-III to another network terminal (e.g., STU-II) through a Gateway. First, the STU-III dials the Gateway. Since the Gateway LIT is strapped for auto-secure, this connection will go secure as described in the STU-III to STU-III call setup. Once a secure connection has been established, the Gateway operator requests from the calling subscriber the called ID and the called phone number. The STU-III user enters the appropriate information and sends a message to the Gateway in the secure dialing or secure voice mode.

selection buttons. If the user initiated the call to transmit secure data through selection of options at the front panel or by depressing a "secure data" button, bits may be set offering one or more of the available data modes. These include bits B5 and B7 in the second byte and bits B3 and B7 in the third byte. One or more of these four bits may be set to indicate the data modes that are being offered. In this case the simultaneous voice/data bit B5 in the third byte, the voice bit B6 in the second byte, and the voice bits B2 and B6 in the third byte shall be set to zero, since at this time the initiator is not offering to enter the simultaneous voice/data mode or the voice mode.

If the user initiated the call to transmit secure voice through selection of options at the front panel or by depressing a "secure voice" button, bits may be set offering one or more of the available voice modes. These include bits B6 in the second byte and bits B2 and B6 in the third byte. One or more of these three bits may be set to "1" to indicate an offer to transmit secure voice in the V.32 mode. Bit B6 in the second and third bytes indicate that the DoD standard 4800 bps voice algorithm will be used to code the voice signal for transmission while bit B2 in the third byte indicates that the Motorola proprietary algorithm will be used. In the case specified by this paragraph, the simultaneous voice/data bit B5 in the third byte, the data bits B5 and B7 in the second byte, and the data bits B3 and B7 in the third byte shall be set to zero, since at this time the initiator is not offering to enter the simultaneous voice/data mode or the data mode.

If the user initiated the call to transmit 4800 bps simultaneous voice/data through selection of options at the front panel, bit B5 in the third byte shall be set to "1". When the simultaneous voice/data mode is offered, the 9600 bps modes shall not be offered. Thus, bits B5 in the second byte, and bits B2 and B3 in the third byte shall be set to "0". The initiator may, however, offer 4800 bps secure voice or 4800 bps secure data, but not both, to offer an optional mode at 4800 bps in case the responder does not have the simultaneous voice/data mode implemented. In offering 4800 bps secure voice as an alternative, the initiator may offer the standard V.32 mode (Byte 2, bit B6), the modified V.32 mode (Byte 3, bit B6), or both. Similarly, the initiator may offer either the standard V.32

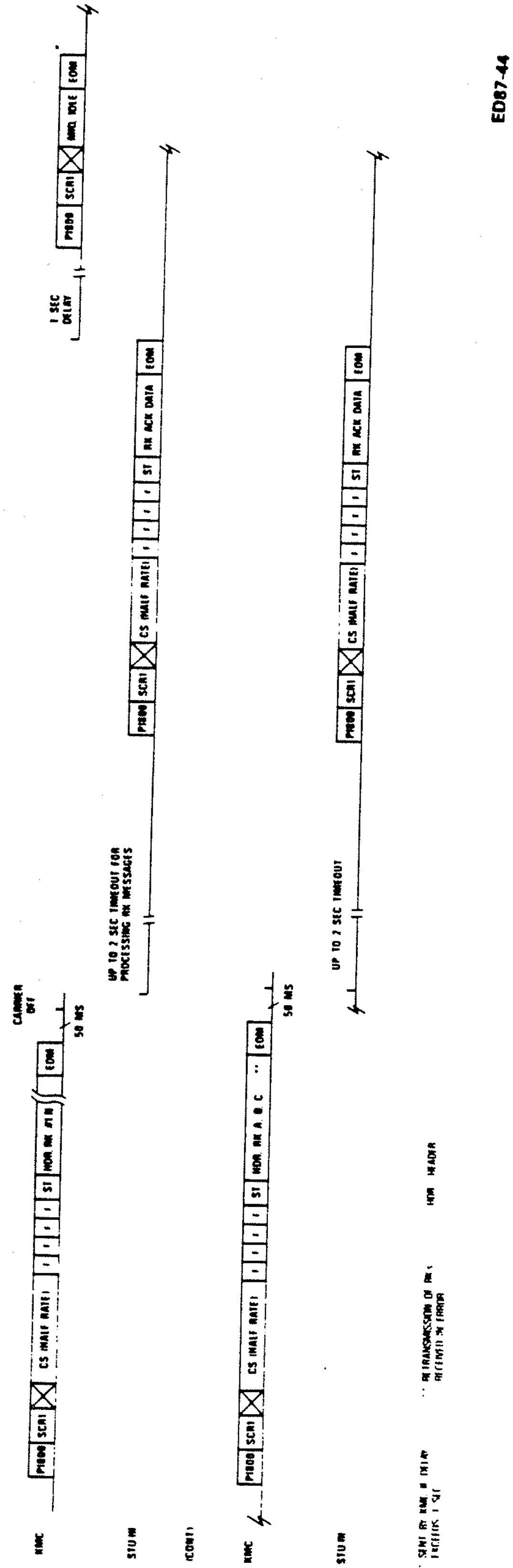


Figure 2-70. KMC/STU-III CKL Signaling Diagram

mode (Byte 2, bit B7), the modified V.32 mode (Byte 3, bit B7), or both when offering 4800 bps secure data as an alternative.

The contents of any additional bytes will be assigned by the Government when required.

2.2.1.2.3 Modulation Format The modulation format for messages A and B shall be that of the Bell 103 modem. This is a 300 baud, continuous phase, FSK format that uses the following frequencies:

	Space	Mark
Initiator:	1070 Hz	1270 Hz
Responder:	2025 Hz	2225 Hz

A specification required for this application, which is not present in the 103 modem, is that the mark and space intervals shall be 1/300 second ± 100 ppm. This will avoid the wide variation in the mark/space intervals that are allowed by the 103 modems.

2.2.1.2.4 Echo Ranging Mode (Optional) If the echo ranging mode is selected by both STU-IIIs, the signaling shall proceed as specified in this section. This section addresses delay estimation only. The remainder of call set-up, including the training of equalizers and near and far-end echo cancellers, is not addressed.

The technique for delay estimation is depicted in Figure 2-7. After a front-end signaling exchange of messages A and B in which it is determined that far-end echo cancellers are to be trained, the responder is silent for a period of 8T, where T = 1/1200 seconds. It then brings up carrier and transmits a dibit sequence of continuous 0s. This produces two tones in the transmitter's output: 1950 Hz and 750 Hz, with the 750 Hz component 33 dB below the 1950 Hz component.

Figure 2-70 provides a timeline for the KMC/STU-III CKL signaling sequence. All STU-III CKL processing is defined in FSVS-220.

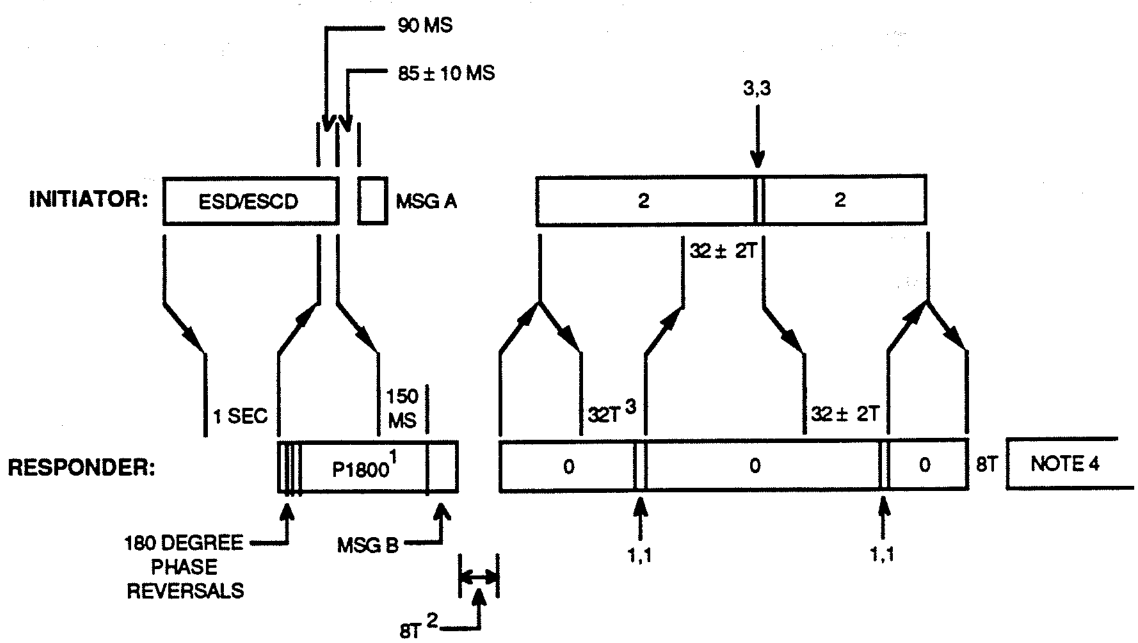
At the conclusion of a successful transfer, the STU-III reenters the KMC Secure Wait state and again monitors the telephone line for another KMC message.

2.3.6 Call Interruption Handling

The signaling design for the STU-III includes provisions for handling resynchronization and call termination. As the KMC front-end functions primarily as an ordinary STU-III, all of the provisions for Release, Failed Call, and Abort signaling and subsequent processing are handled in the same manner as ordinary half duplex STU-III/STU-III interactions, with one possible exception (that is at the discretion of the STU-III terminal designer); once the STU-III enters the KMC secure mode, the STU-III may permit the user to place his handset on hook without terminating the call. If this is done, the terminal shall release the line when the KMC terminates the call, indicated by the STU-III's receipt of the RLS message, other abnormal termination procedures such as ABORT, FAILED CALL, or upon reaching the 10 second timeout waiting for the KMC to respond. If the user decides to terminate the call, he need merely take the handset off-hook, then back on-hook and the STU-III shall initiate the release signaling.

2.4 STU-III INTERACTION WITH OTHER NETWORK ELEMENTS

In addition to operating with a Key Management Center, the STU-III will have to interact with a variety of other network elements. The initial network element to be implemented is a manual (operator-controlled) Gateway between the BELLFIELD (KY-71/KY-72/KY-76) and STU-III terminals. Other elements which may be added subsequently include an automated network gateway, secure conference director, RED enclave PABX or radio/wireline interface. To



Notes:

1. The responder shall continue to transmit P1800 until MSG A is fully received and MSG B is ready. Message B transmission shall begin within 1 second after carrier drop is detected at the completion of MSG A.

2. T = 1/1200 seconds.

3. Maximum of 128T.

4. Next phase of modem training may begin here.

Figure 2-7. Full Duplex Alternate Mode Signaling Diagram
Echo Ranging Mode Selected

2.3.5 Compromised Key List (CKL) Signaling

The KMC will determine whether the STU-III requires a new CKL during the course of the rekey call. The KMC may transmit the CKL before, between or after any RK rekey sets. The CKL message includes an MID and a header, identifying the CKL message and indicating the number of blocks in the message. The CKL message itself is segmented into a number of FIREFLY blocks (CKLi's) as described in Chapter 4. As with the Rekey message, the KMC will precede a CKL message with P1800, 3202, SCR1, SOM, a CS (Half Rate message), four frames of Filler and Start. After receiving the last bit of EOM (or assumed EOM pursuant to the fade processing rules in Paragraph 2.2.5), the STU-III shall allow a timeout of no more than 2 seconds to elapse and then shall respond by transmitting P1800, 3202, SCR1, SOM, a Crypto Sync (Half Rate) message, four frames of Filler, Start, and the CKL ACK message indicating the acknowledged and accepted CKL blocks for the call. Upon reception of the ACK message the KMC shall perform validity checks to verify the ACK message. The KMC shall respond to the ACK message by subtracting the ACKED data (blocks) from the full set of blocks for the message. The balance shall be sent as a new transmission. The KMC may, at its own discretion, terminate the transmission of the CKL and continue the rekey call with the transmission of the rekey sets. The terminal shall not consider this as abnormal and shall continue with the call.

In the case where the terminal has sent a CKL ACK message in response to a garbled first message from the KMC, both the KMC and the terminal shall not consider this as a valid start of the CKL transmission sequence and a later transmission of the CKL shall be treated as valid.

The initiator, which had been silent after transmitting message A, detects the responder's signal, brings up carrier and transmits a dibit sequence of continuous 2s. The initiator's transmit signal is also a pair of tones, but at 1650 Hz and 2850 Hz, where the 2850 Hz component is 33 dB below the 1650 Hz component.

When the initiator's repetitive dibit 2 sequence reaches the responder, the responder must detect it, and then insert two dibit 1s in its dibit 0 transmit signal and start a delay timer. The last two events should occur at a nominal time of 32 symbol periods (32T) and a maximum of 128 symbol periods (128T) after the true arrival time of the initiator's sequence. Note that the time constant of the responder's detector is included in the 32T ± 2T period. The two dibit 1s cause a 180 degree phase shift in the responder's 1950 Hz component.

When the responder's phase shift propagates to the initiator, it is detected. After a 32T ± 2T delay from the arrival of the phase shift, the initiator inserts two dibit 3s in its repetitive dibit 2 transmit signal and starts a delay timer. As with the responder, the detection time is included in the 32T ± 2T delay. The two dibit 3s cause a 180 degree phase shift in the initiator's 1650 Hz component.

When this phase shift arrives at the responder, the responder's delay timer is stopped. Again, after a delay of 32T ± 2T from the arrival of the phase shift, the responder inserts two dibit 1s in its transmit data sequence. This new phase shift is detected at the initiator which causes the initiator's delay timer to stop and transmit carrier to be removed. The responder detects the loss of carrier from the initiator and then begins the next phase of modem training after a silent interval of 8T seconds. Using this technique derived from the CCITT V.32 recommendation, the initiator and responder are now able to independently estimate the round-trip propagation delay of the connection.

2.2.1.2.5 Alternate Mode Selection of Rec. V.32 Interoperable Modem Figure 2-8 illustrates the call setup sequence used to enter one of the interoperable modes for full duplex transmission using the Rec. V.32 modulation format. As

For purposes of the transmission protocol, the STU-III, upon receiving each transmission, shall check its validity as described here and in FSVS-220, and set the appropriate ACK bits in the ACK message for validated blocks. Failure of any of the checks shall be reason for not accepting (ACKing) the RK blocks. If the terminal cannot add any new information to the RK ACK message then the last sent ACK message shall be transmitted in response to a traffic message. The terminal shall also resend the last ACK message for any other error conditions or unexpected transmissions not specifically enumerated elsewhere as a condition for Failed Call. In the case where the first message is garbled as to its type the CKL ACK message can be used. In addition the failure of some of the checks may cause the terminal to enter the Failed Call state.

The reception of the CKL message before or between the Rekey messages shall not affect the RK ACK message.

When the KMC receives the RK ACK, it will determine if any of the RKs were not received properly. Upon reception of the ACK message the KMC shall perform validity checks to verify the ACK message. The KMC shall respond to the ACK message by subtracting the ACKED data (blocks) from the full set of blocks for the message. The balance shall be sent as a new transmission. When a complete vector set has been received and accepted by the STU-III and the KMC has received positive acknowledgment for all blocks in that vector set, the KMC continues with the next vector set transmission. All STU-III Rekey processing is defined in FSVS-220.

At the conclusion of a successful Rekey transfer, the STU-III reenters the KMC Secure Wait state and again monitors the telephone line for another KMC message.

shown, the initiator willing to enter one of the interoperable V.32 modes shall initiate the call setup sequence with the ESCD echo suppressor/canceller disable tone. The responder which is capable of and willing to diverge from the V.26 interoperable 2400 bps mode shall provide the standard alternate mode signaling by inserting the phase reversals at the beginning of the P1800 response. On detecting these phase reversals the initiator that wants to diverge to a V.32 interoperable mode shall provide the standard Message A response indicating the V.32 modes it is offering for use. If the responder does not have one of the V.32 modes offered or otherwise wishes to revert to the V.26 interoperable 2400 bps mode, it shall transmit Message B with the interoperable 2400 bps mode bit set in the first byte and continue transmission in accordance with Figure 2-5. If the responder wishes to diverge to one of the V.32 modes offered, it shall transmit Message B setting a single bit to indicate the mode selected. The bits corresponding to other modes shall be set to zero. After the initiator receives Message B indicating that the V.32 mode has been accepted, it shall assume the role of the "call mode modem" specified by CCITT Rec. V.32. As indicated by Figure 2-8, the initiator shall begin by transmitting carrier state A and continue through the end of the Bl sequence as specified by paragraph 5.4.1 of Rec. V.32. After the responder has transmitted Message B, it shall assume the role of the Answer mode modem of Rec. V.32. As indicated by Figure 2-8, it shall stop transmission for 75 ± 20ms after Message B and resume by transmitting alternate carrier states A and C and continue through the end of the Bl sequence as specified by paragraph 5.4.2 of Rec. V.32.

During the segments of Rec. V.32 indicated by Notes 2 and 3 in Figure 2-8, the initiator and responder shall conform to the specification of Rec. V.32 in all respects unless the "modified" V.32 mode has been selected during the Message A/B exchange. When the modified rules for modem training have been selected, both the initiator and the responder shall transmit a minimum of 7424T symbols of the TRN sequence for all occurrences of TRN. In addition, if a training failure is detected prior to the completion of the B1 sequence the modem detecting the failure shall initiate a modem retrain in accordance with

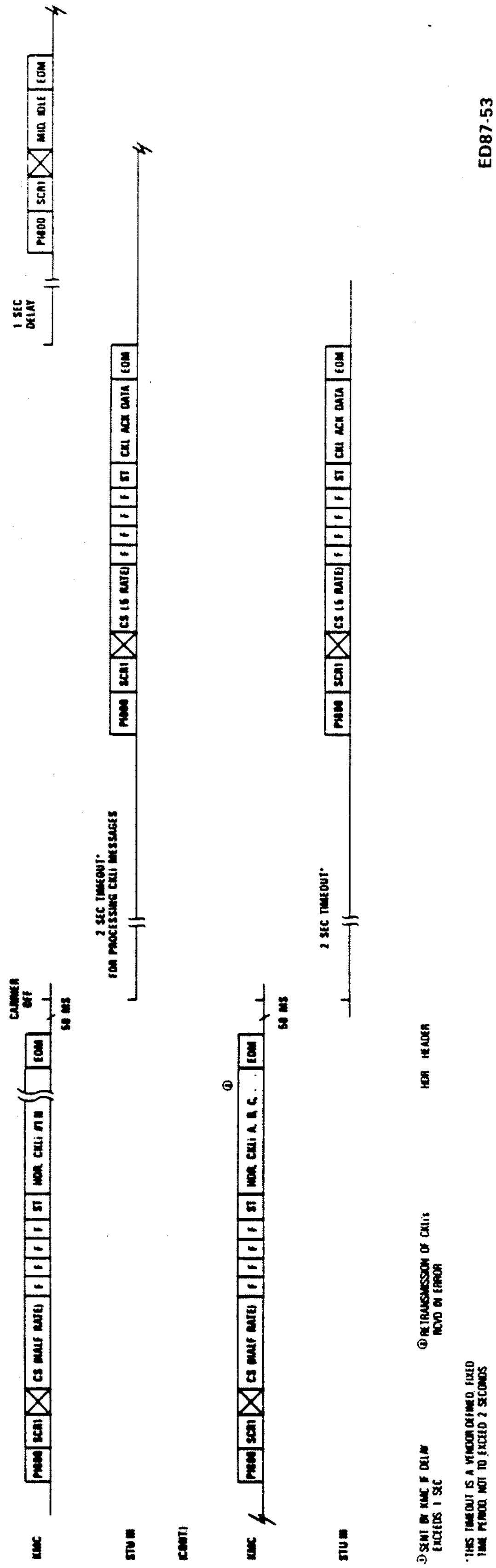
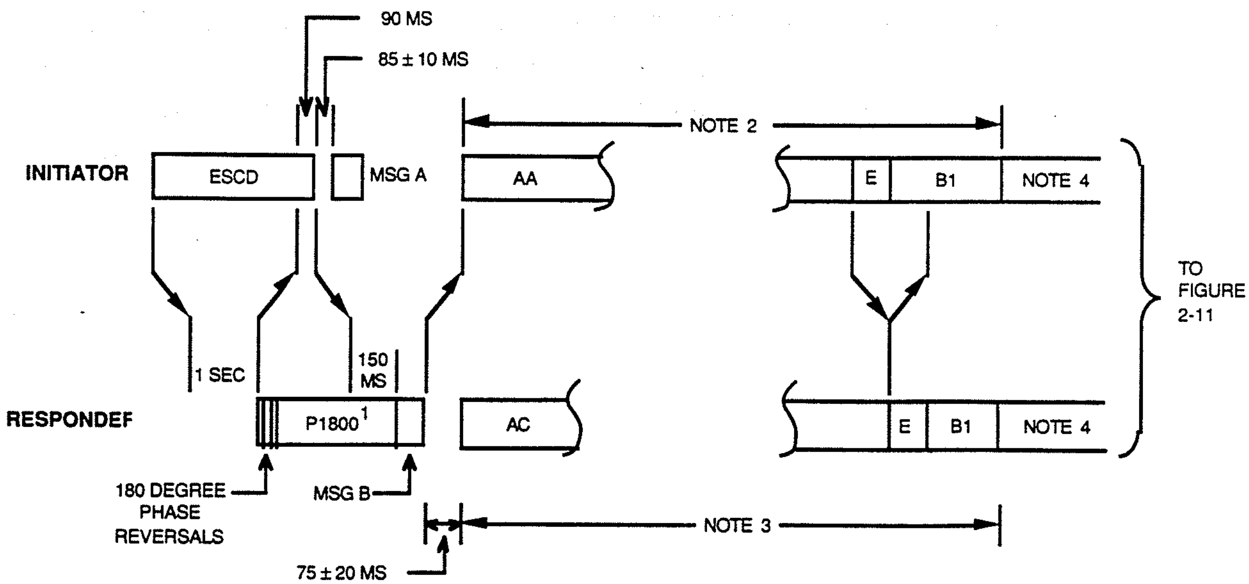


Figure 2-69. KMC/STU-III Rekey Signaling



Notes:

1. The responder shall continue to transmit P1800 until MSG A is fully received and MSG B is ready. Message B transmission shall begin within 1 second after carrier drop is detected at the completion of MSG A.

2. In the region indicated by Note 2, the Initiator shall follow the line signaling specified for the Call mode modem of V.32, paragraph 5.4.1.

3. In the region indicated by Note 3, the Responder shall follow the line signaling specified for the Answer mode modem of V.32, paragraph 5.4.2.

4. Immediately following the Bl sequence, transmission shall continue with the SOM, CAP/SV sequence shown in Figure 2-11.

Figure 2-8. Full Duplex Alternate Mode Signaling Diagram V.32 Mode Selected

There is a header field that includes the number of RKs being sent. The STU-III is capable of handling up to 8 RKs sent in consecutive order (e.g., RK1, RK2, RK4, ..., RK8). The message is followed by an unencrypted EOM and drop of carrier within 50 ms. The detailed message formats and content of the messages are provided in Chapter 4. There are two possible FIREFLY II formats that could be implemented in the STU-III design. Depending on whether the terminal requires Format 1 or Format 2 material, the KMC transmits up to eight RK blocks for one vector set of a FIREFLY rekey. The detailed format and content of all messages exchanged in the KMC/STU-III signaling are contained in Chapter 4. The content of the RK messages is different for Format 1 than for Format 2 and for full security material than for unclassified material as indicated in Chapter 4.

After receiving the last bit of EOM (or assumed EOM pursuant to the fade processing rules in Paragraph 2.2.5), the STU-III shall allow a timeout of no more than 2 seconds to elapse and then shall transmit the Rekey ACK message indicating the status of the individual RK blocks of all received rekey messages. This time represents a maximum processing time required by the STU-III for decoding and processing any of the RK blocks. The RK ACK message is preceded by P1800, 3202, SCR1, SOM, CS Half Rate Data (HDX), four frames of Filler, Start and the RK ACK messages itself. The format and content of the RK ACK message is provided in Chapter 4. Depending on the FF format selected, up to eight of the dibits may be filled for a FIREFLY vector set transfer.

The ACK message is a continuing history of the present REKEY call. The terminal shall initialize all variable fields of the ACK message to "0" at the start of the Rekey exchange. In response to the received traffic messages, the terminal shall incrementally fill in the ACK message as the call continues with the edition numbers of the Rekey messages, as shown in Table 2-6.22, appearing in the order they were received.

the V.32 retraining rules described in Rec. V.32, paragraph 5.5. In other respects the standard and modified V.32 rules are identical. Additional details of the modes within this sequence are specified in Section 2.2.3 covering operation in the V.32 mode.

Following the completion of the Bl sequence, the responder and initiator shall turn off the scramblers specified by Rec. V.32 and continue with the call setup protocol beginning in Figure 2-11 using the V.32 modulation format selected. Transmission of the SOM in Figure 2-11 shall follow immediately after the end of the Bl sequence.

2.2.1.3 Full Duplex Variable Exchange

The second phase of call set-up is performed by the two STU-IIIs, with no actions required by the users; it consists of the full duplex exchange of the status and FIREFLY protected messages required to establish a cryptographic variable for the call. Figure 2-9 depicts the overall signaling during this phase. FSVS-220 contains the specific processing requirements for each message exchanged in this phase of call set-up.

Exchange Capability/Status Vector. The initiator and re-sponder terminals exchange Start of Message (SOM) and Capability/Status Vector (CAP/SV), where CAP/SV is a message containing the STU-III Type (I or II), the STU-III manufacturer code, a Government ID code, secure dialing status, BERT status, and FIREFLY status information.

The FIREFLY status data is contained in four fields, each indicating the availability of a FIREFLY vector set. Based on this status information, each terminal will independently select the most recent edition of the highest class of FIREFLY keying material which is common to both terminals. This material will be used for the remainder of the variable exchange signaling. Figure 2-9 is a flow diagram describing the signaling-related functions necessary for the CAP/SV exchange. Separate flows are included for both the transmission and messages to determine what has been successfully received and accepted by the terminal.

The KMC shall terminate a call with a RELEASE message only if it has successfully received an ACK for all of the keysets it intended to send. The successful completion of a CKL is not necessary for the KMC to send a RELEASE message.

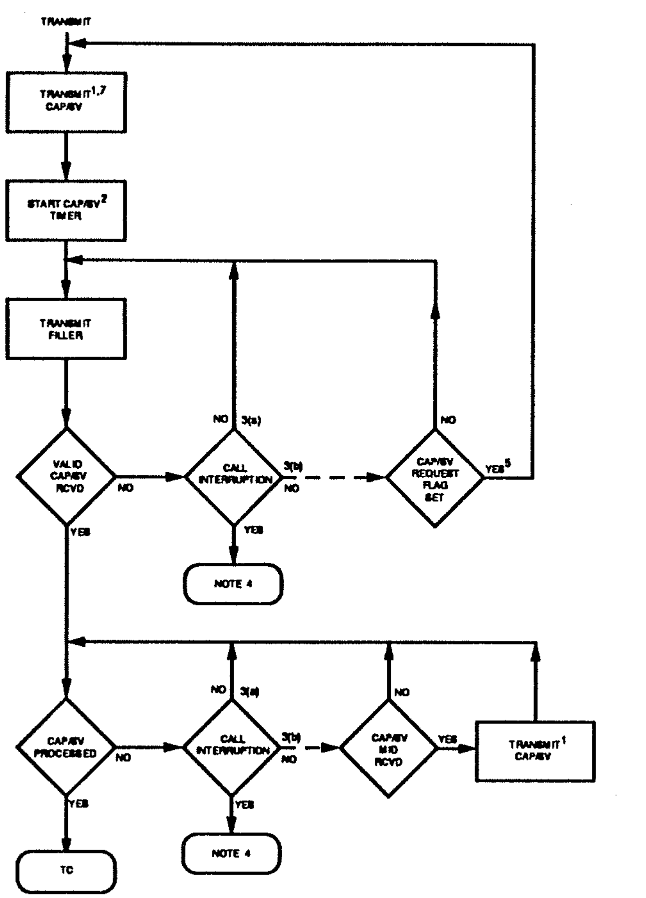
2.3.3.2 Exception Processing

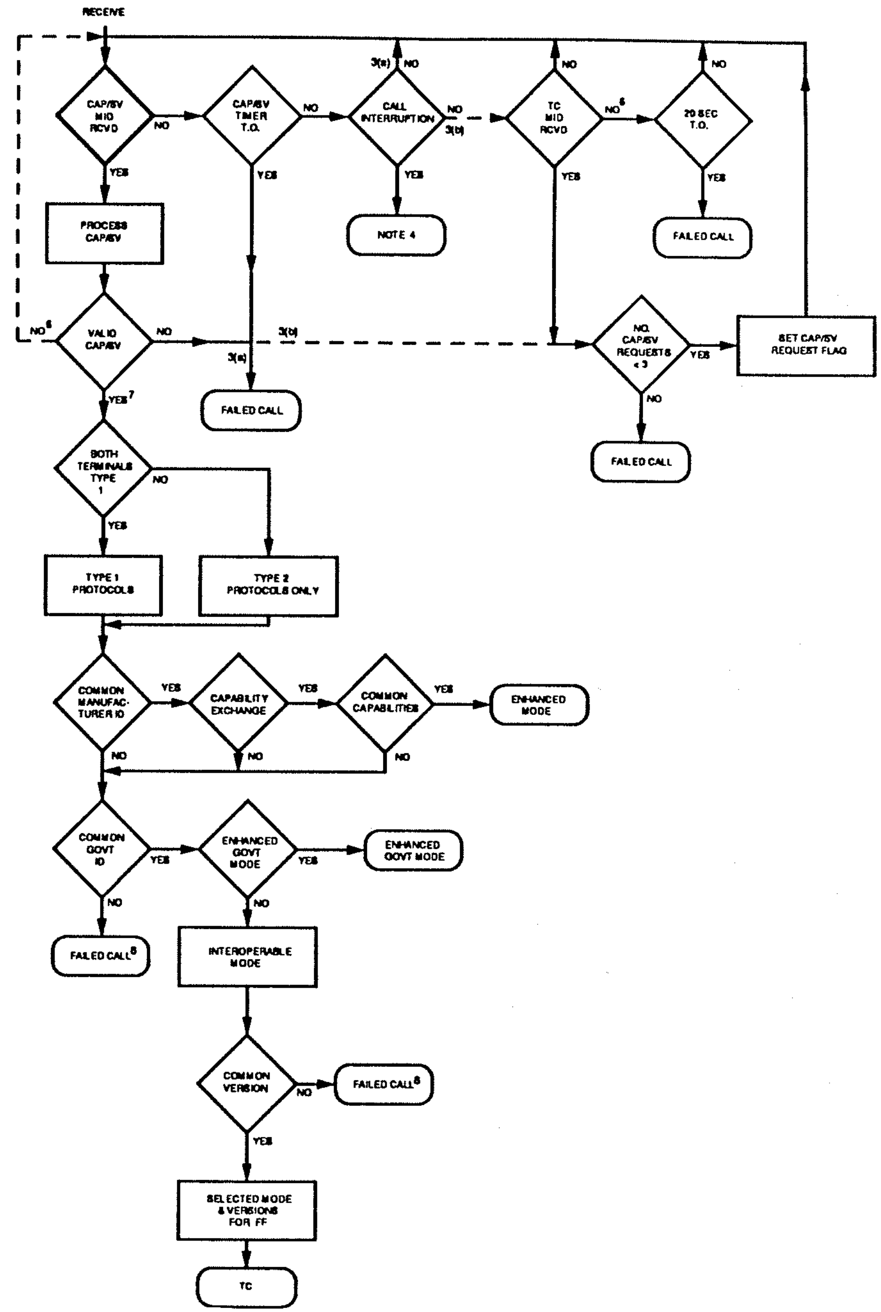
In the case of the first message from the KMC being garbled to the point where no intelligent ACK message can be built, the STU-III shall return a CKL ACK message with all fields showing a "0" state. The transmission of the CKL ACK message for this reason shall not be considered as a valid transmission or reception of the CKL message such that it would cause the STU-III to not accept the real CKL message later in the call.

After transmitting a traffic message, the KMC shall cease transmission and wait for either the returned traffic message (ACK) or a minimum 10 second time out. The timer is canceled upon the recognition of the traffic type message. Upon reaching the timeout the KMC may fail the call. The KMC is responsible for terminating the call in the event of irrecoverable faults due to excessive retransmissions.

2.3.4 Rekey Message Processing

Type I, Full security STU-IIIs can receive both new full security keying material, and new unclassified keying material. The KMC is responsible for determining which keying material is to be sent to a particular STU-III. The STU-III must be able to accept any keying material update provided by the KMC. Figure 2-69 provides a timeline for a typical KMC/STU-III Rekey signaling sequence. The Rekey message processing for all materials required by a STU-III from the KMC is described below.





Notes:

1. Terminals with retransmission protocol are subject to the transmit delay requirement of Section 2.2.1.3.1.7.
2. Per Table 2-1 or 2-2.

3(a). Path taken by terminals without retransmission protocol.
3(b). Path taken by terminals with retransmission protocol.

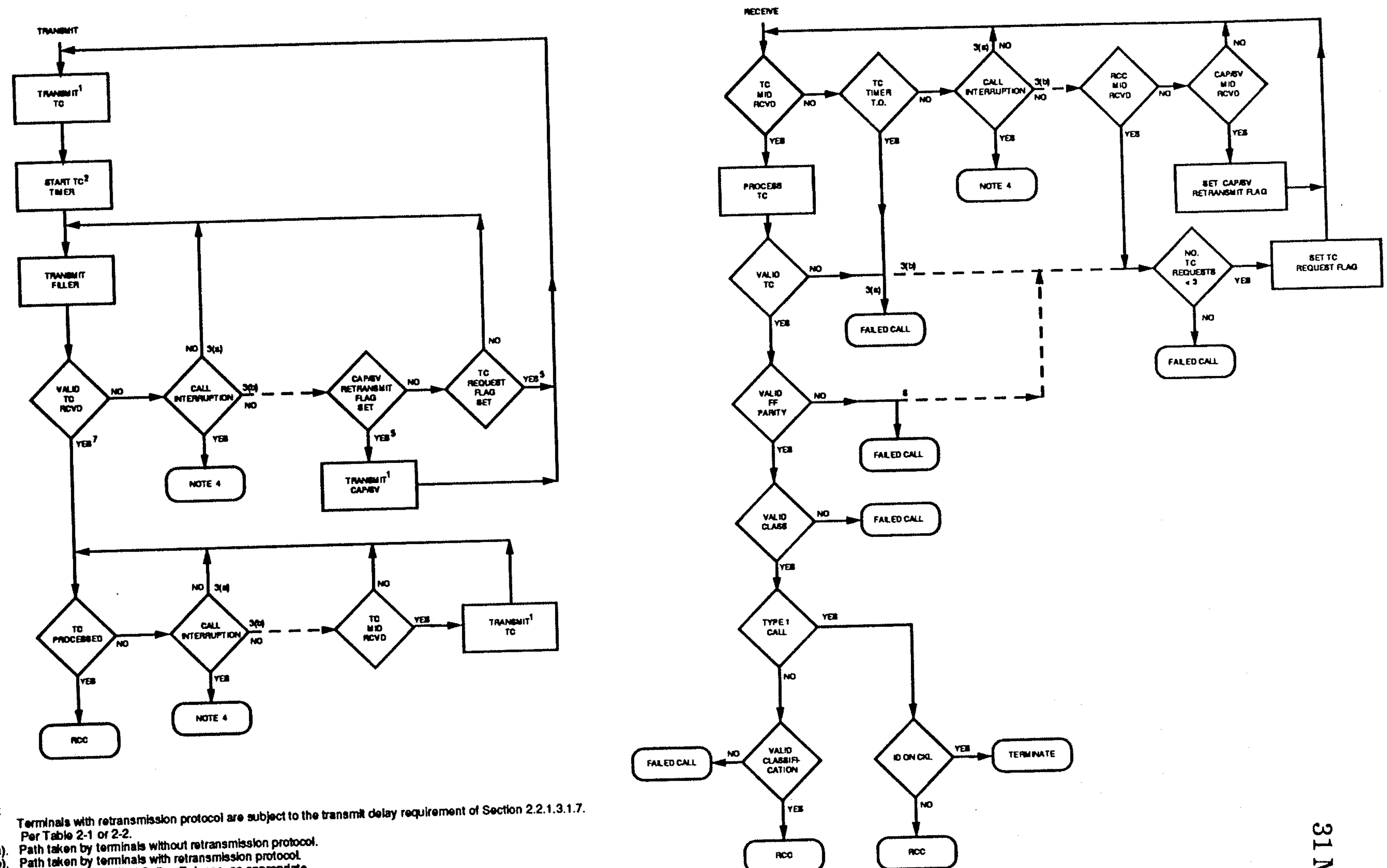
4. Process Abort, Failed Call or Release, as appropriate.
5. Clear flag on exit to "Yes" branch.
6. Negative branch for 2400 bps responder with retransmission protocol. Other terminals take alternate negative branch.
7. 2400 bps responder with retransmission protocol delays transmission of CAP/SV until valid CAP/SV received. During delay terminal transmits Filler or continues SCR1.
8. The terminal shall complete the TRANSMIT CAP/SV segment of this flow diagram prior to transmitting the Failed Call message.

Figure 2-9. CAP/SV Exchange Signaling Sequence Flow Diagram (Initiator and Responder) these blocks. The KMC is not restricted from retransmitting a previously sent and accepted block in the set. The up-to-five data sets (4 rekey sets, 1 CKL) can come in any order.

The STU-III, upon receiving each transmission, shall check the validity of the message for purposes of determining the acceptance of the blocks within the message (set the ACK bits). If any of the checks defined in FSVS-220 fail, the blocks shall not be accepted (ACKed). In addition, the failure of some of the checks may cause the terminal to enter the Failed Call state. If the STU-III receives and verifies a block that it has previously accepted (ACKed), it may either overwrite the old block with the new one or ignore the new one.

Once the KMC starts the transmission of a rekey set, it shall not start a new rekey set or a CKL until the KMC has received an ACK for all of the blocks it expected to send for the set. Transmission of a CKL set, however, may be suspended in an incomplete state to continue the call with rekey sets, send a RELEASE message, or otherwise terminate the call; the STU-III shall not go to a Failed Call state for this condition.

The KMC shall analyze the received data to determine the validity of the message. The validity checks shall include all fixed fields being the values defined in Tables 2-6.22 and 2-6.24, variable fields being only legitimate and expected values. If the message is not valid the KMC shall treat the message as an all "Os" ACK message for the current key set or assume that it was identical to the last accepted ACK message. If the message is determined to be valid, the KMC shall then either retransmit the unacknowledged blocks from the last message, or if all blocks have been ACKed move on to the next set of data to be sent, or terminate the call. Once the KMC has completed transmission of a rekey set, and moved on to another rekey set or the CKL, it shall not resend any blocks of the completed rekey set during the same call. Once the KMC has terminated the transmission of the CKL for any reason it shall not retransmit the CKL later in the same call. The KMC shall only use valid received ACK



Notes:
1. Terminals with retransmission protocol are subject to the transmit delay requirement of Section 2.2.1.3.1.7.
2. Per Table 2-1 or 2-2.
3(a). Path taken by terminals without retransmission protocol.
3(b). Path taken by terminals with retransmission protocol.
4. Process Abort, Failed Call or Release, as appropriate.
5. Clear flag on exit to "Yes" branch.
6. Terminals with retransmission protocol may fail the call on FF parity error, or use a FF parity error as a basis for requesting retransmission.
7. Terminals requesting retransmission on FF parity error exit this branch when valid FF parity is declared.

Figure 2-10. TC Exchange Signaling Sequence Flow Diagram (Initiator and Responder)

Both the Rekey and CKL messages from the KMC are preceded by a CS Half Rate Data (HDX) message sequence followed by at least four frames of Filler, Start and the KMC traffic message. Once half-duplex, half-rate, data-mode cryptosync has been attained, both the STU-III and the KMC shall respond as if they had received a rekey (or CKL) traffic message. If the STU-III receives a transmission from the KMC and does not achieve half-duplex, half-rate, data mode cryptosync, it shall remain in the KMC secure wait state, as shown in Figure 2-68.

Based on the concurrence of the header and MID information on the first received block which passes BCH parity, the STU-III shall determine whether the message is a CKL or RK message and send the appropriate CKL or RK ACK message. If the STU-III cannot determine the received message type, it shall resend the previous ACK message; if the first message received during a Rekey Session cannot be identified, the STU-III shall send a blank CKL ACK message. In response to a received message, the KMC shall determine the validity of the ACK message by performing consistency checks on the message received and then take the appropriate action for the next step in the call. As a minimum the KMC shall reset any timers associated with the waiting for a message and start timers associated with the transmission requirements for KMC WAIT or traffic messages.

2.3.3.1 Normal Rekey Call Transmission

Once the call has reached the traffic state, the KMC shall start transmission of one of up-to-five possible data sets (rekey sets or CKL). A rekey set is defined as some number of RK blocks which, when combined with the information currently stored in the terminal shall provide the terminal with a usable keyset. The first transmission of each rekey set (or CKL set) shall contain the entire set of data (RK or CKL blocks) that will be sent for that rekey set (or CKL). Any subsequent transmissions for this message will be this set or a subset of receipt of the CAP/SV message. The design of the signaling requires that both the initiating and responding terminals perform the transmit and receive functions concurrently as depicted in the figure.

Exchange FF Identity Vectors. Each set of FIREFLY key material includes a Local Terminal Cipher (LTC). The LTC is sent to the remote terminal. A flow diagram for the LTC exchange is provided in Figure 2-10.

In a similar manner, the remote terminal sends its LTC. This received message is designated as the Remote Terminal Cipher (RTC). The RTC is then FF decrypted.

Once this message is received, the STU-III performs a variety of checks on the data. These include checks of the embedded parity, the class, the classification, the key ID, and the expiration date.

Upon receipt of this message, a Type I terminal will compare the given key ID with the terminal's most recent Compromised Key List (CKL). If the key ID is found in the CKL, the call is terminated. If the other terminal is a Type II, or if the key ID is not found in the CKL, the call setup continues.

The process of call setup to this point is summarized in Figure 2-11. This is the timeline for the exchange of status vectors and terminal capability messages. The filler messages are transmitted while processing is taking place in the STU-III.

Exchange Call Variable Components. The next step in the call setup procedure is the generation and exchange of Random Component Cipher (RCC) messages. A flow diagram for the RCC exchange is provided in Figure 2-12. The terminal forms the local RCC or Local Random Component Message (LRCM). This message contains information related to the crypto variable, a Compromise Information Message (CIM) and Terminal Serial Number for Type I terminals only, and parity on the message. The message is FIREFLY-

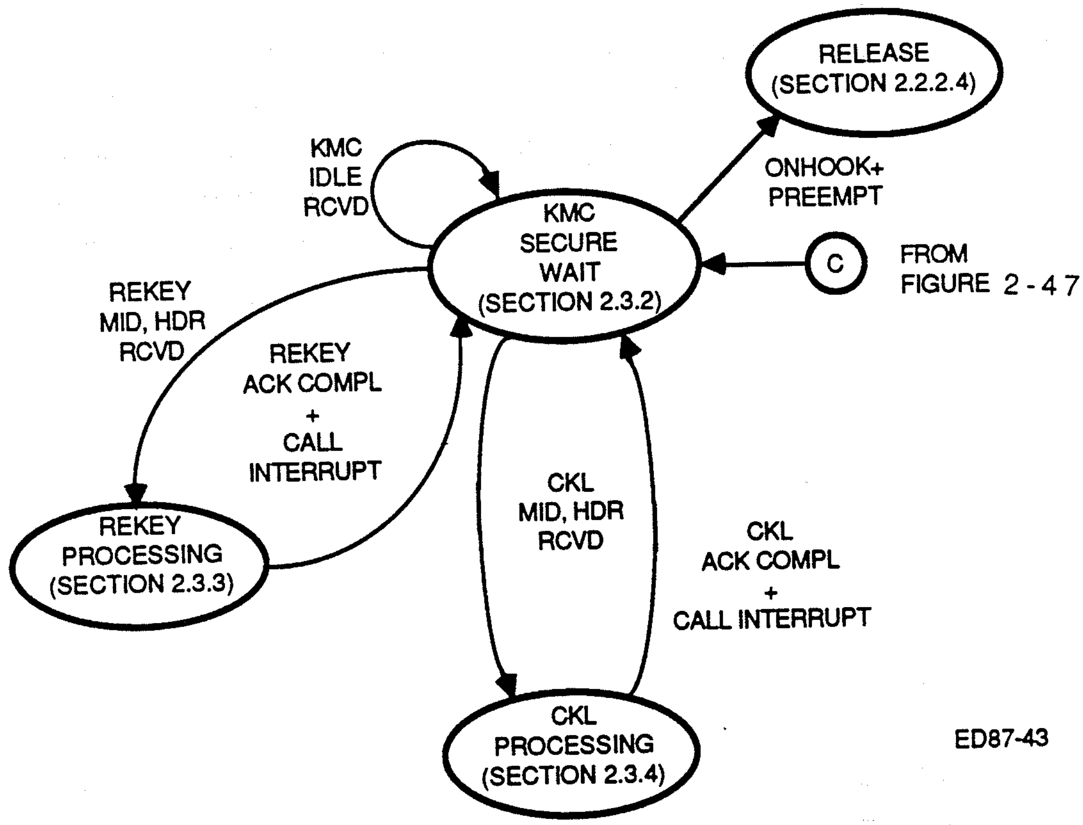


Figure 2-68. KMC Secure Wait Processing Sequence Flow Diagram

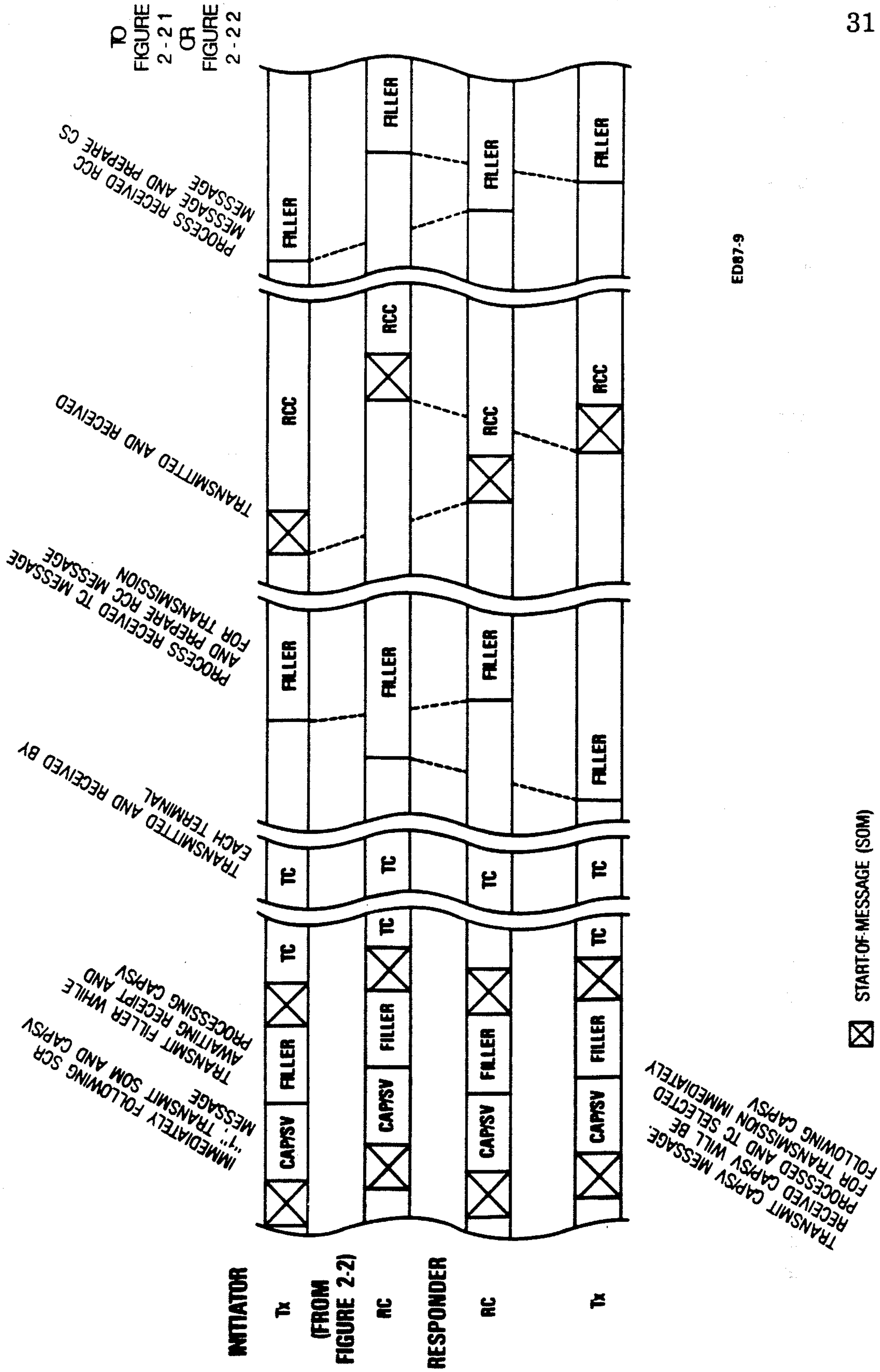
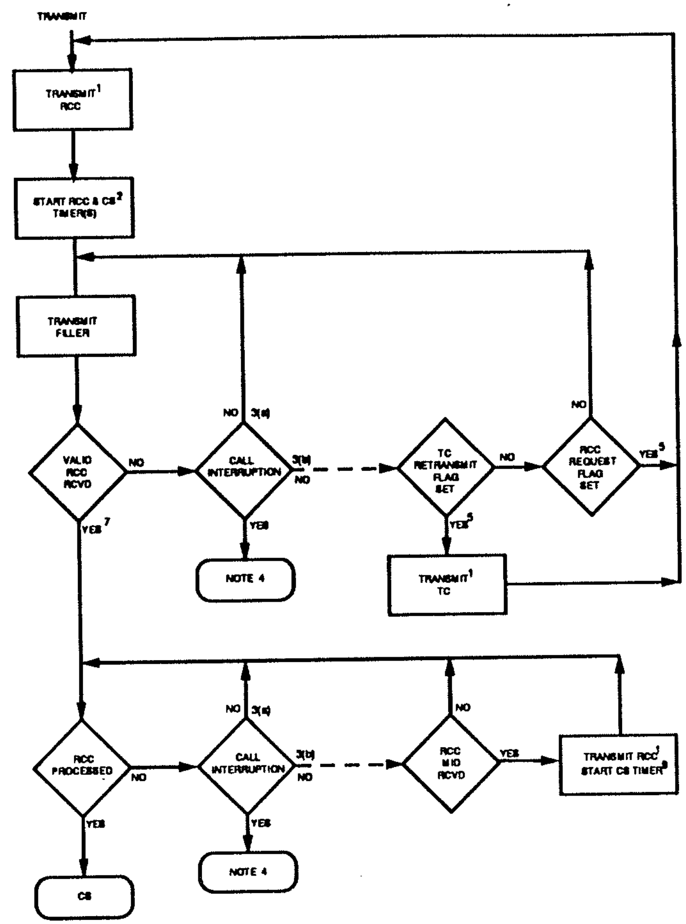


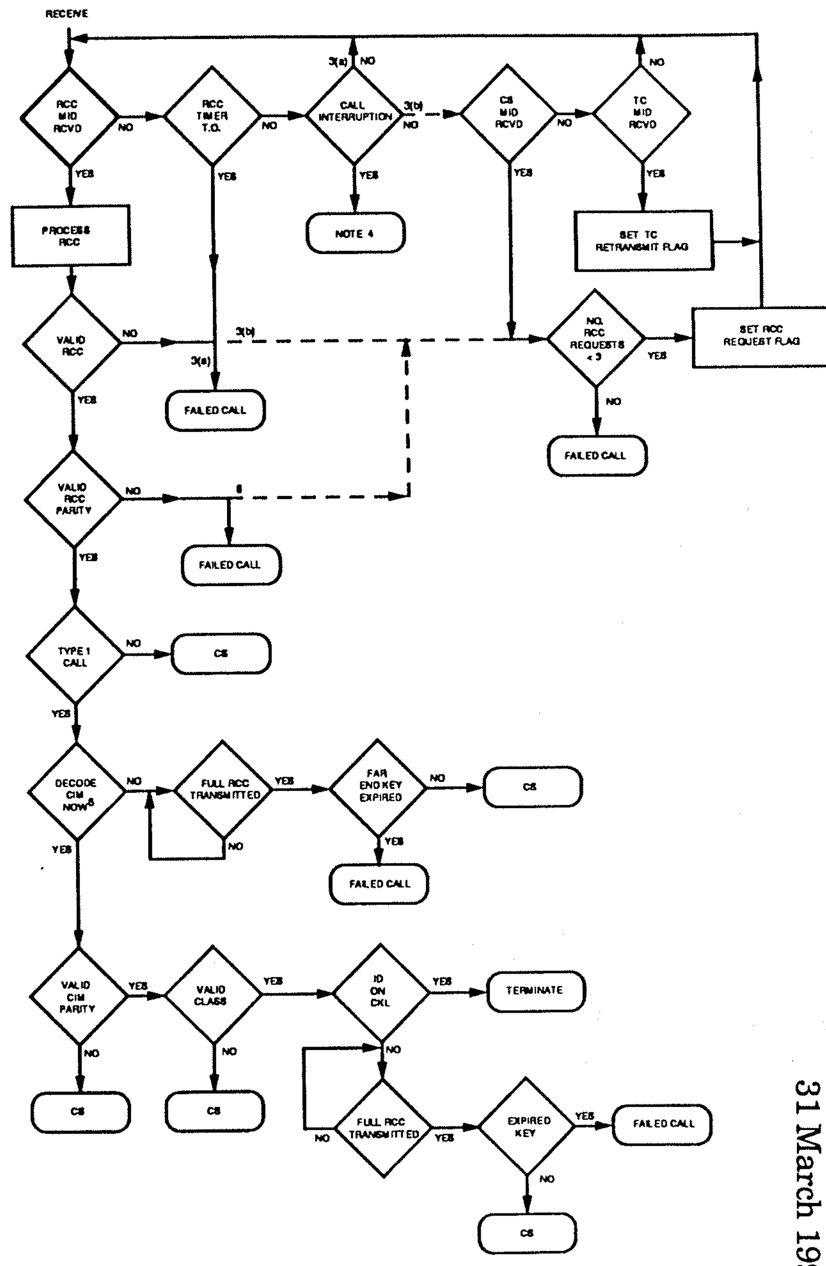
Figure 2-11. Full Duplex Variable Exchange Signaling Diagram

Interaction between the STU-III and KMC includes the half duplex transfer of rekeying messages and/or the CKL, as well as transfers of acknowledge messages from the STU-III to the KMC. All of these transfers are performed using an encrypted/plaintext (E/P), BCH coded message structure. All information is segmented into 128 bit blocks and encrypted appropriately. Each encrypted block is then BCH coded, (using the same BCH (255, 131) code used during the Variable Exchange and Crypto Sync phases of the call setup), and then transmitted using the 2400 bps half duplex modem. The effective information transfer rate for any information between the KMC and STU-III is 1200 bps. The BCH coding is performed on the encrypted data prior to transmission.

2.3.3 KMC Processing Secure Wait

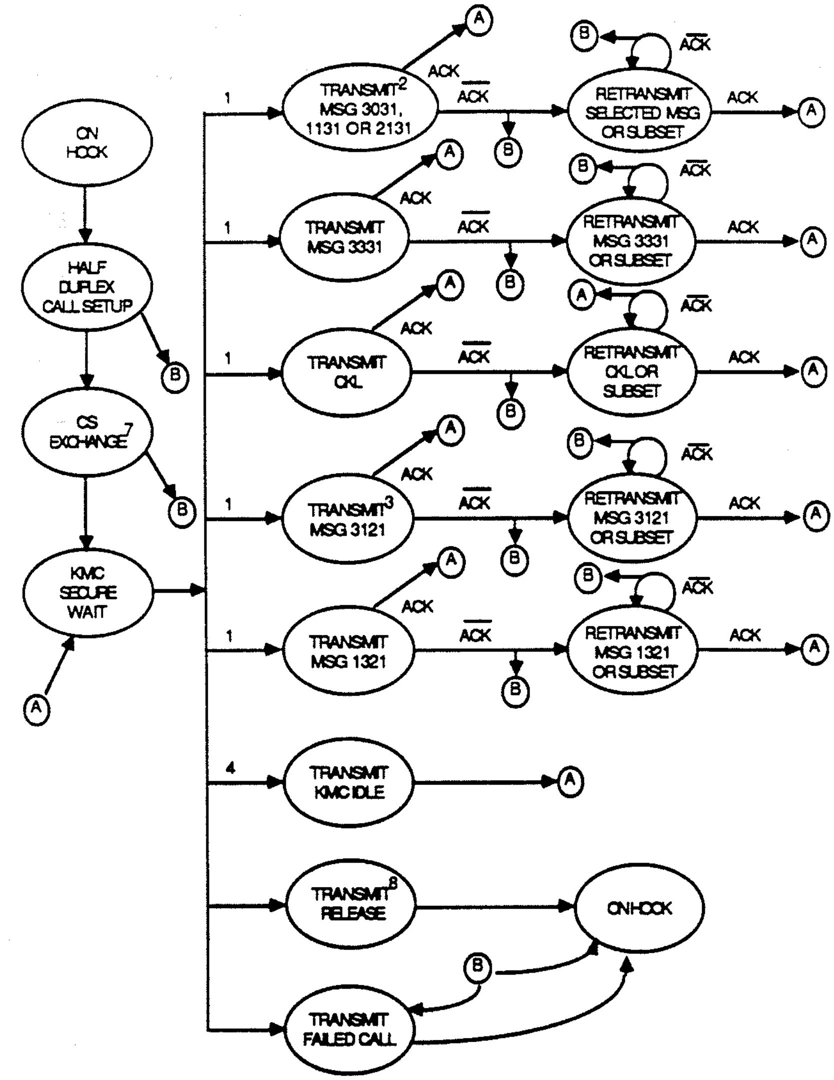
When either the front-end KMC terminal or the STU-III is not transmitting, it enters the secure wait state, as depicted in Figure 2-68. As shown in the state transition diagram, the terminal remains in this state until the STU-III receives a KMC traffic message (i.e., Rekey or CKL) or an indication of KMC processing delay or call termination. All secure messages between the STU-III and KMC start with the normal half duplex transmission sequence (i.e., P1800, 3202, SCR1, and SOM). If the KMC encounters delays in excess of three seconds while performing internal processing of messages for the STU-III, the KMC will transmit a non-data-bearing IDLE message at a nominal three second intervals (as defined in Chapter 4) to provide an indication to the terminal that the line is functioning properly and that the KMC is still connected to the line. There is no restriction, other than limitations imposed by the Half Duplex protocol, as to how soon after a KMC WAIT message that the traffic message can follow. Release processing is performed compatible with normal half duplex call sequences. This can be initiated by the KMC, by the user terminating the call, or by the STU-III not receiving a KMC response for a ten second timeout.





Notes:
1. Terminals with retransmission protocol are subject to the transmit delay requirement of Section 2.2.1.3.1.7.
2. Per Table 2-1 or 2-2.
3(a). Path taken by terminals without retransmission protocol.
3(b). Path taken by terminals with retransmission protocol.
4. Process Abort, Failed Call or Release, as appropriate.
5. Clear flag on exit to "Yes" branch.
6. Terminals with retransmission protocol may fail the call on FF parity error, or use a FF parity error as a basis for requesting retransmission.
7. Terminals requesting retransmission on FF parity error exit this branch when valid FF parity is declared.
8. Optional, CIM processing may be delayed until after call completion.
9. Per Table 2-2.

Figure 2-12. RCC Exchange Signaling Sequence Flow Diagram (Initiator and Responder)



NOTE 1: These states may be entered only once, but may be entered in any order.

2: Message 3031 may not be transmitted if the message 3331 is transmitted during call.

3: Message 3121 must be transmitted if message 1321 is transmitted during call.

4: KMC will enter this state at nominal 3 second intervals, if other messages are not ready for transmission.

5: The messages 1131, 2131 and 3121 identified above are for calls from a Format 1 STU-III. These are replaced with messages 1231, 2231 and 3221 respectively when the calling STU-III uses Format 2 keying material.

6: The KMC may also transition to "B" on a timeout waiting for any ACK shown above.

7: This CS exchange shall use the MID for CS Half Rate Data (HDX).

8: Release is transmitted only if the KMC has entered the "Transmit Msg" state for all Rekey and CKL messages intended for the call.

Figure 2-67. KMC Rekey Call State Transition Diagram encrypted and is sent to the other terminal while a similarly generated message is received and decrypted.

The received message is designated the Remote Random Component Cipher (RRCC). This message is also referred to as a Random Component Cipher (RCC). Figure 2-11 shows the timeline for the exchange of the RCC messages.

Once this message has been received from the remote terminal, and it is BCH decoded and decrypted, the terminal will process the RCC message. The terminal will first check the embedded parity of the overall message. If the parity is incorrect, the terminal will enter Failed Call processing. Otherwise, the terminal uses the information contained in the received RCC to create the per call traffic variable.

If the call is between two Type I terminals, the STU-III will process a CIM contained within the RCC message. The CIM requires additional processing so it can be used to update the stored Compromised Key List (CKL). The STU-III design has the option of processing the CIM at a later time, for example, at call termination. (If this processing is done during call set-up, the time for call set-up could increase). If the CIM is not processed at this time, the STU-III will check the key expiration date of the received TC against the stored CIM after the LRCM and RRCC have been fully exchanged. If the far-end key has expired, the STU-III will enter the Failed Call state. After the CIM is itself decrypted, the terminal checks the CIM message parity and the class. If either test fails, the terminal skips the CKL update. If the STU-III decodes the CIM and updates the CKL during the secure call set-up, the STU-III shall then perform checks of parity, class, key ID, and key expiration date of the far-end terminal against the new CKL information. If the received parity or class is invalid, the terminal shall skip the CKL update. If the key ID of the far-end terminal is on the CKL, the terminal shall enter the Release state. If the key expiration date received in the RTC is older than the date in the new stored CIM, terminal shall enter the Failed Call state after it has transmitted the full LRCM either test fails, the terminal skips the CKL update. If the STU-III the KMC shall wait for an ACK message. In the event that the first transmission of a message is unsuccessful, the KMC shall either fail the call or retransmit the message. In retransmitting the message, the KMC shall restransmit all of the RK blocks in the first transmission or a subset of them as determined necessary by the KMC. When a retransmission is necessary, the first 4 dibits of the MID and the Edition No. will remain unchanged. If a subset of the original message is transmitted, the BCH Block Count, No. RK Blocks and Block Status field will be adjusted to correspond to the RK blocks being retransmitted. The state transitions permitted during this transmission and retransmission process are defined in Figure 2-67.

2.3.2 STU-III/KMC Call Set-Up

The STU-III/KMC calls will be half duplex using the same general call set-up protocols (i.e., procedures for modem initiation/training, variable exchange, and crypto-sync sequences) used for half duplex calls between STU-IIIs. The protocols for the transfer of information between the STU-III and the KMC are addressed in this section.

The call setup for the STU-III/KMC interaction during the POTS, initial call/modem training and variable exchange phases are identical to the STU-III/STU-III interaction described in Section 2.2.2. The front-end terminal at the KMC will be strapped for Auto-Secure. Although the STU-III places the call to the KMC, the KMC front-end initiates the secure call setup signaling assuming the role of the Initiator. The variable exchange is completed in the same manner as for two STU-IIIs in half duplex operation. When the FF exchanges are completed, and a per call variable has been established, the KMC terminal will send Rekey and/or CKL messages as described in the paragraphs below.

decodes the CIM and updates the CKL during the secure call set-up, the STU-III shall then perform checks of parity, class, key ID, and key expiration date of the far-end terminal against the new CKL information. If the received parity or class is invalid, the terminal shall skip the CKL update. If the key ID of the far-end terminal is on the CKL, the terminal shall enter the Release state. If the key expiration date received in the RTC is older than the date in the new stored CIM, terminal shall enter the Failed Call state after it has transmitted the full LRCM.

2.2.1.3.1 Full Duplex Retransmission Protocol for Call Setup Enhancement STU-IIIs may, as an option, incorporate automatic protocols to repeat modem training and call setup messages in accordance with the provisions of this section. Terminals implementing the option shall implement all of the provisions in this paragraph. The implementation of the optional features shall be done in such a way that no deviations are taken to the standard call setup sequence unless a failure in the standard sequence has occurred.

2.2.1.3.1.1 Modem Training Retries If call setup fails during the training sequence for the 2400 bps modem, a terminal detecting a failure shall abort the modem training sequence and cease transmitting. After detecting a failure, the responder shall set a 10 second timeout, return to the idle condition and wait for the initiator to restart the call setup sequence. If the 10 second timeout expires the responder shall abort the call setup attempt and prompt the user to activate a nonsecure control to reenter the analog mode. The initiator of the original Full Duplex signaling sequence shall pause three seconds after ending its transmission and then initiate the call setup sequence again.

Both terminals shall allow three attempts (including the initial attempt) to complete the training sequence. If the third try is unsuccessful, the terminal shall abort the call setup attempt and prompt the user to activate a nonsecure control to reenter the analog mode.

Table 2-7. Rekey Call Message Combinations - Format 2 Terminal

MID	Rekey Message Contents	Rekey Call Message Combinations																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
3031	UDM_L, LTC_L (existing TEM)		*						*						*				
3331	UDM_L, LTC_L (new TEM)					*	*					*	*					*	*
1231	UDM_L, LTC_L UN_L			*			*			*			*			*			*
2231	LTC_L, UN_L				*	*					*	*					*	*	
3221	UDM_S, LTC_S, UN_S							*	*	*	*	*	*	*	*	*	*	*	*
1321	UDM_S, LTC_S, (new TEM)													*	*	*	*	*	*

If call setup fails during the training sequence for the V.32 modem, the terminal response is specified in Section 2.2.3.1.6.

2.2.1.3.1.2 Responder's Transmission of CAP/SV at 2400 bps When the retransmission protocol is implemented, the responder's sequence in the 2400 bps mode after the transmission of the 704 bits of SCR1 shall be determined by the quality of the received CAP/SV, as specified below.

If the initiator's CAP/SV is received and decoded so that it successfully passes any validity checks imposed by the terminal, the responder shall transmit the SCR1/SOM/CAP/SV sequence and continue with the standard signaling plan. If the initiator's CAP/SV is not received, or fails the validity checks, the responder shall complete the specified 704 bits of SCR1 and then either continue SCR1 or transmit Filler. The responder shall continue transmitting Filler or SCR1 until it receives a valid CAP/SV or times out. Following receipt of a valid CAP/SV, the responder shall resume the full duplex signaling sequence by transmitting SOM/CAP/SV. This signaling sequence is illustrated in Figure 2-13.

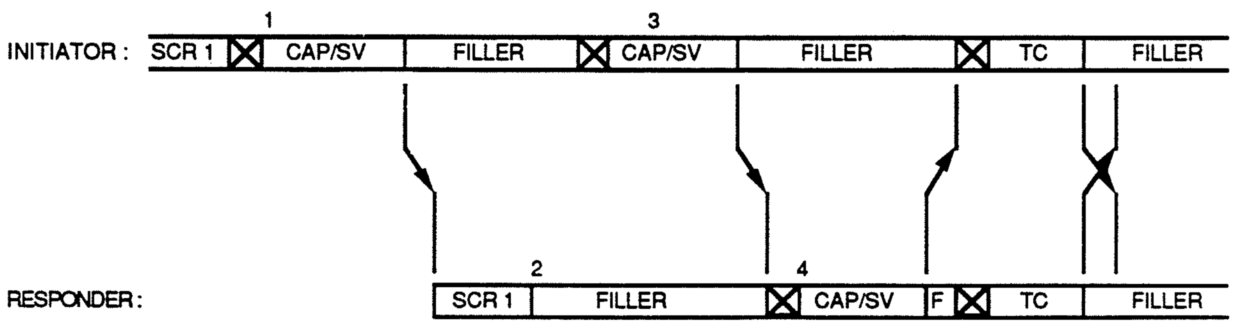
2.2.1.3.1.3 Retransmission Request for CAP/SV, TC and RCC Messages
Except as specified above for the 2400 bps responder, a STU-III may explicitly request retransmission of the CAP/SV, TC, or RCC messages by transmitting its own version of the message requested in accordance with the following rules:

(1) A message in the process of transmission shall be completed prior to the start of the retransmission request,

(2) The retransmission request shall be sent where Failed Call would otherwise be sent,

Table 2-6. Rekey Call Message Combinations - Format 1 Terminal

MID	Rekey Message Contents	Rekey Call Message Combinations																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
3031	UDM_L, LTC_L (existing TEM)		*						*						*				
3331	UDM_L, LTC_L (new TEM)					*	*					*	*					*	*
1131	UDM_L, LTC_L UN_L			*			*			*			*			*			*
2131	LTC_L, UN_L				*	*					*	*					*	*	
3121	UDM_S, LTC_S, UN_S							*	*	*	*	*	*	*	*	*	*	*	*
1321	UDM_S, LTC_S, (new TEM)													*	*	*	*	*	*



Notes:

1. Initial Transmission of CAP/SV.

2. Responder detects uncorrected error in CAP/SV and sends Filler (or continues SCR1) in lieu of Failed Call.

3. Initiator Repeats CAP/SV as a retransmission request for CAP/SV.

4. Responder receives CAP/SV correctly and resumes 2400 bps Full Duplex sequence by transmitting CAP/SV followed by TC.

Figure 2-13. Full Duplex Retransmit Sequence Responder Request for CAP-SV (V.26 Mode only) rekey call. In all other cases, the KMC shall transmit, at most, one message associated with the long vectors during a rekey call. This may be the UDM_L, LTC_L (existing TEM), the UDM_L, LTC_L, UN_L or the LTC_L, UN_L message. Alternatively, the KMC may send no message associated with the long vectors. (2) The KMC shall transmit the short vector message identified as UDM_S, LTC_S (new TEM) only in conjunction with a UDM_S, LTC_S, UN_S message transmitted during the same rekey call. The KMC may, alternatively, transmit a UDM_S, LTC_S, UN_S message by itself, or may send no messages in the short vector category.

Within these two rules, there are 18 combinations of Rekey messages that may be sent to a terminal during a Rekey call. These combinations are identified in Tables 2-6 and 2-7 for Format 1 and Format 2 terminals respectively. Each column in Table 2-6 and 2-7 represents a legitimate combination of messages that may be transmitted during a single rekey call. An asterisk in the column indicates that the message will be included in the rekey call for that combination. The KMC shall select for the Rekey call one of these 18 combinations of messages appropriate to the Format 1 or Format 2 terminal, depending on the rekey state of the system and the terminal.

In addition to one of the Rekey message combinations selected from Tables 2-6 and 2-7, the KMC may transmit a CKL message, as described in Section 2.3.5.

2.3.1.3 State Transitions Followed by the KMC

Although the KMC shall control the progress of the Rekey call, it shall be limited by the state transition constraints described in this section. As discussed in the previous section, the KMC shall select a combination of Rekey and CKL messages to transmit to the terminal. The CKL and Rekey messages selected by the KMC may be transmitted to the terminal in any order, and in different orders on different calls, as determined by the KMC to minimize the overall KMC line holding time. After transmitting a message to the terminal,

(3) If three retransmission requests for the same message are sent and an error free version of that message is not received within the specified timeout, the terminal shall transmit Failed Call or Restart Failed Call;

(4) A retransmission request shall not be transmitted for a message already received correctly;

(5) Until a valid CAP/SV is received, any received TC or RCC messages shall be ignored, and

(6) Until a TC message is received error free, any received RCC messages shall be ignored.

2.2.1.3.1.4 Processing of Received Messages As an option terminals may correct errors in the received CAP/SV, TC, or RCC messages by using information from similar messages received earlier in the same call setup sequence. The terminal may replace BCH blocks with uncorrectable errors with the corresponding good blocks from previous transmissions, or may perform two out of three voting on a bit wise basis if three copies of the same message are available.

2.2.1.3.1.5 Retransmission Request Processing After receiving an error free copy of a CAP/SV, TC or RCC message from the remote terminal, the STU-III shall regard any additional call setup messages received with the same MID as requests for retransmission of the message identified by the MID. The remainder of the received message shall be ignored. After receiving a retransmission request, the STU-III shall transmit a copy of the message requested in accordance with the following rules:

(1) A message in the process of transmission shall be completed prior to the start of the retransmission;
(2) A response to a request for retransmission shall take precedence over the transmission of any other call setup messages;

Table 2-5. Rekey Message Contents

MID	NO. RK BLOCKS	PER RK BLOCKS	CONTENTS[2]	TABLE
3031 dddd[1]	4	RK 1, 2, 3, 4	UDM_L, LTC_L(existing TEM)	2-6.17
3331dddd[1]	4	RK 1, 2, 3, 4	UDM_L ,LTC_L (new TEM)	2-6.17
1131 dddd[1]	5	RK 1, 2, 3, 4, 5	UDM_L ,LTC_L ,UN_L (Format 1)	2-6.17
2131 dddd[1]	3	RK 3, 4, 5	LTC_L, UN_L, (Format 1)	2-6.17
1231 dddd[1]	8	RK 1, 2, 3, 4, 5, 6, 7, 8	UDM_L ,LTC_L , UN_L (Format 2)	2-6.18
2231 dddd[1]	6	RK 3, 4, 5, 6, 7, 8	LTC_L , UN_L (Format 2)	2-6.18
1321 dddd[1]	2	RK 1, 2	UDM_S , LTC_S (new TEM)	2-6.19
3121 dddd[1]	3	RK 1, 2, 3	UDM_S , LTC_S ,UN_S (Format 1)	2-6.19
3221 dddd[1]	4	RK 1, 2, 3, 4	UDM_S , LTC_S , UN_S (Format 2)	2-6.20

[1]See Note 1 In Table 2-6.8.

[2]UN_L (Format 1) refers to the terminal unique rekey material in Format 1 for the long vectors. Similarly, UN_L (Format 2) refers to the terminal unique rekey material in Format 2 for the long vectors. The subscripts "L" and "S" denote rekey material for the long and short vectors respectively.

(3) Requests for retransmission received from the remote terminal shall be honored without limit on the number of retransmissions, and

(4) In conjunction with the transmission of the requested message, the terminal shall back up in the call setup sequence to the point prior to the requested message and repeat the call setup sequence from that point.

Figures 2-14 through 2-19 illustrate the retransmission request and response sequences.

2.2.1.3.1.6 Call Interruption Processing STU-III terminals with the retransmission protocol shall generate and respond to all call interruption messages. No deviations are implied to the call interruption specifications by the retransmission protocol option. This specifically requires the terminals performing call setup at 4800 bps to follow the restart failed call sequence after the retransmission protocol limits have been exceeded.

2.2.1.3.1.7 Transmission Delay After Uncorrected Transmission Errors When the STU-III detects an uncorrected transmission error in a received message, it shall delay the start of transmission of any new message for at least 1.25 seconds after the time the error occurred. During the delay the terminal shall complete the transmission of any message in progress and then transmit Filler.

2.2.1.3.1.8 Timeouts for Terminals Implementing Retransmission Protocol The timeouts specified in Table 2-1 shall be replaced by those specified in Table 2-2 for terminals implementing the retransmission protocol. Where Figures 2-9, 2-10, 2-12 and 2-20 refer to timeouts per Table 2-1 or 2-2, terminals implementing the retransmission protocol shall use the timeouts specified in Table 2-2. Other terminals shall use timeouts from Table 2-1. As shown in Table 2-2, timeouts set on the final bit of SCR1 and at the start of P1800 apply only to the 2400 bps mode. When the signaling for a call has changed to the V.32 mode, terminals shall disregard these timeouts.

the state transitions that it may follow in transmitting and retransmitting messages to the STU-III from the beginning to the end of the rekey call. These constraints are described below in Section 2.3.1.1, 2.3.1.2, and 2.3.1.3, respectively.

2.3.1.1 Messages Transmitted by the KMC

There are nine rekey messages and 1 CKL message which the KMC may transmit to convey rekey and CKL information to a terminal. The messages are defined in Tables 2-5 and 2-6.8. In selecting messages for transmission, however, the KMC shall not send messages identified as "Format 1" to a Format 2 terminal, nor shall the KMC send messages identified as "Format 2" to a Format 1 terminal.

The detailed message structure of the messages associated with the MIDs 1131, 1231, 3121 and 3221 is shown in Tables 2-6.17, 2-6.18, 2-6.19, and 2-6.20, respectively. The remaining messages are subsets of these as indicated by the RK blocks to be transmitted. As indicated in the more detailed description, the first BCH Block contains information to indicate the contents of the remaining BCH blocks in the message. The MID contains the message type and the BCH block count field as described in Table 2-6.8. The Edition No. will be filled in by the KMC to indicate the edition number of the universal corresponding to, or contained in, the message being transmitted. The No. RK Blocks and Block Status fields indicate how many and which RK blocks are contained in the remainder of message.

2.3.1.2 Message Combinations Transmitted by the KMC

The total set of rekey messages transmitted to a STU-III during a single rekey call shall be limited by the following rules: (1) The KMC shall transmit the long vector message identified as UDM_L, LTC_L (new TEM) only in conjunction with an LTC_L, UN_L or UDM_L, LTC_L UN_L message transmitted during the same

2.2.1.3.1.9 Use of Filler with Retransmission Protocol Terminals may transmit Filler before or after messages transmitted as part of the retransmission protocol. No minimum or maximum amount of Filler is specified. Terminals may transmit messages without intervening Filler at the option of the implementation.

2.2.1.4 Full Duplex Cryptosync/Resync

The third phase of call set-up includes the exchange of Crypto Synchronization (CS) messages between the STU-IIIs during initial synchronization and subsequent resychronization when required. This section addresses two major operations:

- Initial sychronization from a clear to a secure call

- Resychronization either within the same mode (following an out-of sync condition) or to a new mode

During each of these operations, the cryptographic variable will not be changed (i.e., the terminal will use the variable resulting from the Variable Exchange phase). The phase has three functions: to coordinate the selection of the secure mode; to exchange the initialization data necessary to align each terminal's receive KG to the far-end transmit KG; and to coordinate the start of the secure mode traffic (for both transmit and receive). Cryptosync processing is specified in FSVS-220; only the specific signaling sequences for each of these operations is discussed below.

A CS message in the full duplex mode must be followed by at least four frames of Filler to allow the far end terminal to be ready to receive traffic, however, in the data mode, Start is sent only after the data is available for transmission. A Start message is transmitted just prior to the first bit of traffic.

2.3 (TYPE I) STU-III/KEY MANAGEMENT CENTER (KMC) INTERACTION

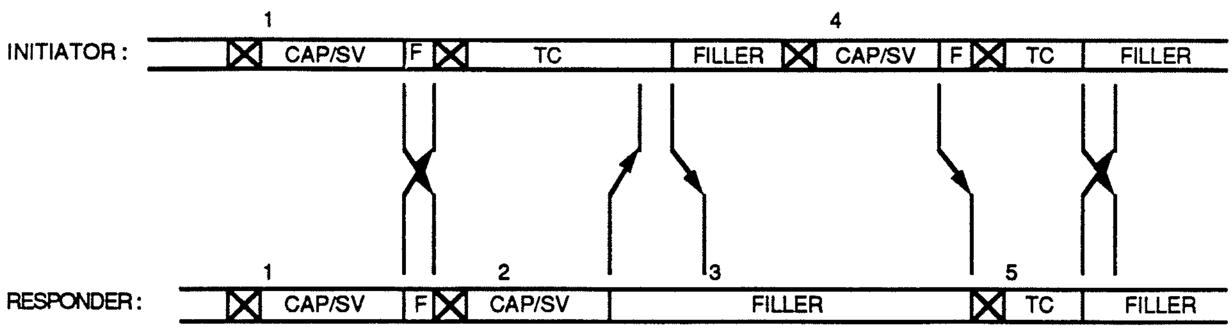
This section provides the requirements for the interaction between the KMC and the STU-III during a rekey call.

The requirements imposed on the KMC are described in Section 2.31. The call setup between the KMC and the STU-III is described in Section 2.3.2. When the STU-III "goes secure", it enters a Secure Wait state which is described in Section 2.3.3. The normal rekey call transmission process is described in Section 2.3.3.1, while Section 2.3.3.2 discusses exceptions to the normal process. When the STU-III receives a rekey or CKL message it enters the rekey or CKL processing state as described in Sections 2.3.4 and 2.3.5, respectively. Resynchronization and the procedures for terminated calls are discussed in Section 2.3.6. Detailed message formats and additional requirements for the STU-III's use and storage of information received are contained in FSVS-220, the Terminal Performance Specification.

2.3.1 KMC Requirements During a Rekey Call

The STU-III user will call the KMC to rekey the terminal or obtain a new Compromised Key List (CKL). After answering the call, the KMC shall initiate the secure call setup and shall determine what information, if any, to send to the terminal. During the remainder of the call the KMC shall interact with the STU-III in a master/slave relationship.

The KMC shall operate as master and control the progress of the call. The KMC shall provide information to the STU-III by transmitting a series of rekey and/or CKL messages. The messages shall be sent as data using a half duplex, half rate data transmission protocol as shown in Figure 2-69 and 2-70. During the rekey call the KMC shall operate within three rules that constrain: (1) the individual messages which it may send to a terminal, (2) the combinations of messages which it may send to a terminal during a single rekey call, and (3)



Notes:

1. Initial Transmission of CAP/SV.

2. Responder detects uncorrectable error in CAP/SV and sends Retransmit CAP/SV Request in lieu of Failed Call.

3. Responder discards received TC since CAP/SV has not been received correctly.

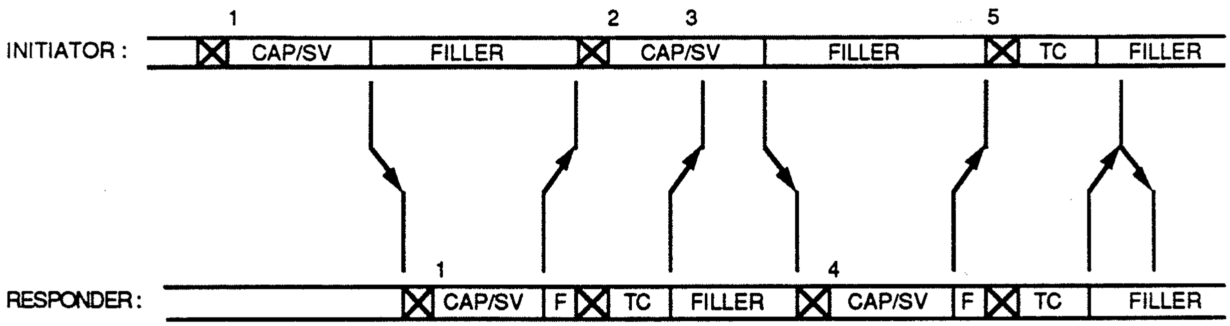
4. Initiator completes TC transmission and backs up to transmit CAP/SV state, transmits CAP/SV and repeats TC.

5. Responder receives CAP/SV correctly and resumes V.32 Full Duplex sequence by transmitting TC.

Figure 2-14. Full Duplex Retransmit Sequence Responder Request for CAP-SV (V.32 Mode only) transmitter for a minimum of one second after detecting the fade. If the line signal returns within the one second, the terminal shall continue to process the line signal without a resynchronization. If the line signal does not return within the one second interval, the terminal will assume that it "missed" the EOM flag, enable the transmitter and resume normal half duplex operation in which case the user may initiate a new transmission. The STU-III shall continue to bridge modem baud sync for a minimum of five seconds unless the user initiates a transmission within the five second time period. Termination of the call (or reversion to a plaintext analog call) is left to the discretion of the users.

2.2.6 Digital Network (56/64 Kbps) Operation

(TO BE SUPPLIED LATER)



Notes:

1. Initial Transmission of CAP/SV.
2. Initiator detects uncorrectable error in CAP/SV and sends Retransmit CAP/SV Request in lieu of Failed Call.
3. Initiator discards received TC since CAP/SV has not been received correctly.
4. Responder completes TC transmission and backs up to transmit CAP/SV state, transmits CAP/SV and repeats TC.
5. Initiator receives CAP/SV correctly and resumes Full Duplex sequence by transmitting TC.

Figure 2-15. Full Duplex Retransmit Sequence Initiator Request for CAP/SV (V.26 or V.32 Mode)

Variations in output due to all causes may exceed the nominal tolerances by +/- 2.5 dB if the 2.5 +/-2 dB nominal difference in amplitude of the frequencies in the high and low groups is maintained. Therefore the amplitude of any frequency in the high group will always be at least 0.5 dB higher, but not more than 4.5 dB higher, than any frequency in the low group.

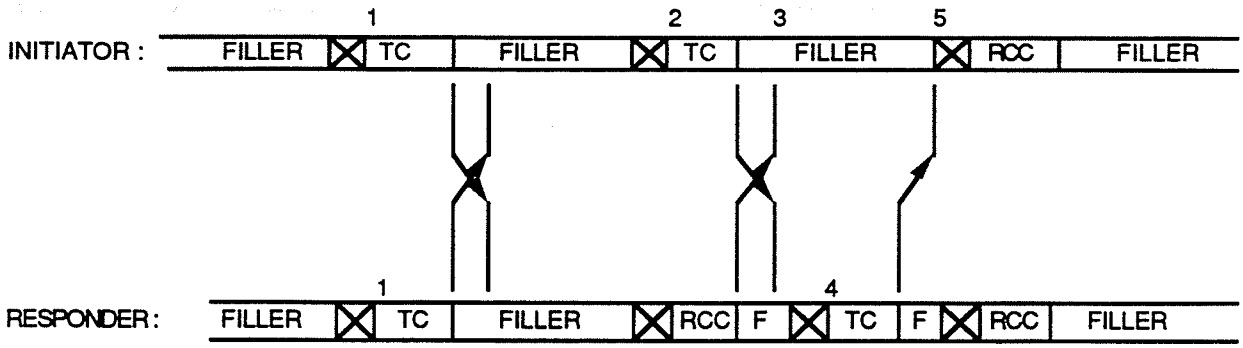
B. Dial Pulse Signaling. Dial pulse signaling is not required on the 4-wire AUTOVON interface.

C. Preemption. The STU-III AUTOVON, while operating in a secure mode over the standard 4-wire interface, shall meet the requirements defined in Section 2.2.4.1 for AUTOVON preempt detection.

2.2.5 Cellular Radio Operation

Several of the STU-III terminal designs will be capable of being configured for operation over a cellular radio network. These terminals will be directly interoperable with STU-IIIs connected to the standard telephone network. The STU-III shall be capable of detecting a fade (loss of carrier), defined below, and shall be capable of bridging modem baud sync for a minimum of five seconds when a fade condition exists. In the full duplex mode, detection of loss of carrier, unexpectedly, constitutes a possible fade condition. In the half duplex mode, detection of loss of carrier without detection of an EOM first, constitutes a possible fade condition. If a fade occurs in either the half or full duplex modes, the STU-III shall detect the loss of carrier and maintain timing to permit operation immediately (without crypto or modem resynchronization) when the line signal returns.

One additional feature is required for half duplex operation to handle a situation where a transmission fade occurs during an utterance transmission. If the terminal detects loss of carrier without detection of the EOM flag, it will have to initially assume that the far-end terminal may still be transmitting during a fade. In this situation, the terminal will have to disable its



Notes:

1. Initial Transmission of TC.

2. Initiator detects uncorrectable error in TC and sends Retransmit TC Request in lieu of Failed Call.

3. Initiator discards received RCC since TC has not been received correctly.

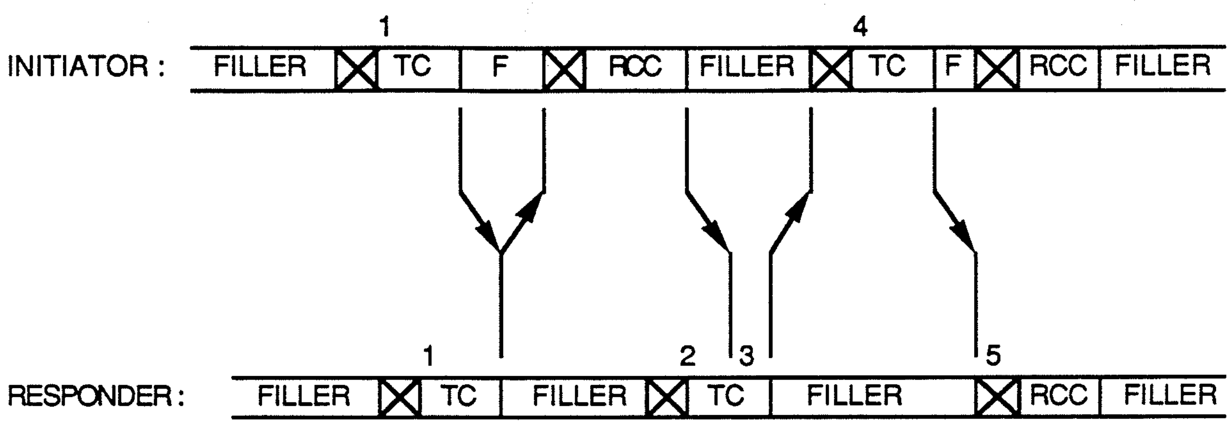
4. Responder completes RCC transmission and backs up to transmit TC state, transmits TC and repeats RCC.

5. Initiator receives TC correctly and resumes Full Duplex sequence by transmitting RCC.

Figure 2-16. Full Duplex Retransmit Sequence Initiator Request for TC (V.26 or V.32 Mode)

Table 2-4. AUTOVON DTMF Tone Frequencies

Signal		DTMF Keys	Frequency - Hz (± 1.3%)
Digit	1	1	697 + 1209
Digit	2	2	697 + 1336
Digit	3	3	697 + 1477
Digit	4	4	770 + 1209
Digit	5	5	770 + 1336
Digit	6	6	770 + 1477
Digit	7	7	852 + 1209
Digit	8	8	852 + 1336
Digit	9	9	852 + 1477
Digit	0	0	941 + 1336
Precedence	(FLASH OVERRIDE)	FO	697 + 1633
Precedence	(FLASH)	F	770 + 1633
Precedence	(IMMEDIATE)	I	852 + 1633
Precedence	(PRIORITY)	P	941 + 1633
		A (#)	941 + 1477
		*	941 + 1209



Notes:

1. Initial Transmission of TC.

2. Responder detects uncorrectable error in TC and sends Retransmit TC Request in lieu of Failed Call.

3. Responder discards received RCC since TC has not been received correctly.

4. Initiator completes RCC transmission and backs up to transmit TC state, transmits TC and repeats RCC.

5. Responder receives TC correctly and resumes Full Duplex sequence by transmitting RCC.

Figure 2-17. Full Duplex Retransmit Sequence
Responder Request for TC (V.26 or V.32 Mode)

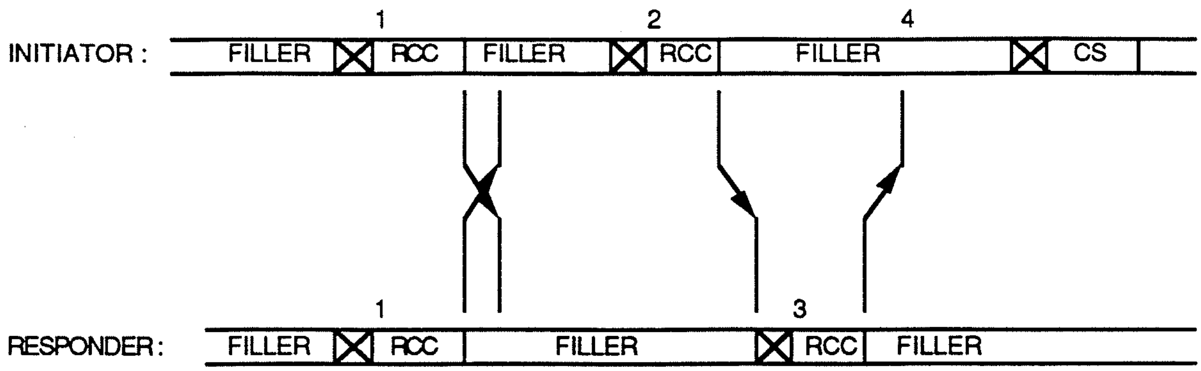
measured at the zero Transmission Level Point (TLP). The STU-III shall be capable of detecting this tone after loss of carrier is detected and before the five second timeout is exceeded, as indicated in Figure 2-33. Upon detection of the preempt tone, the STU-III shall continuously alert the user with a display message (as defined in FSVS-220) and an aural indication (independent of the handset) until the user hangs up.

2.2.4.2 AUTOVON 4-Wire Interface Signaling

The STU-III shall provide the signaling capabilities, as defined below, to interface to the MLPP AUTOVON network using a standard 4-wire interface, as defined in FSVS-220.

A. <u>DTMF Dialing</u>. The STU-III shall provide a means for dialing 16 dial characters. These include four precedence characters (FO, F, I, P) in addition to the normal 12-button commercial telephone dialing pad characters. The telephone line signaling resulting from these four keys will be the transmission of a tone pair on the station transmit line. The tone pair will result from combining one frequency from a high group and one from a low frequency group in a fashion similar to that of the normal two-wire network. Table 2-4 defines the frequencies for each of the 16 dial characters. The transmitted DTMF tones must be within +/- 1.3 percent of the nominal frequency listed. Nominal output levels for the DTMF tones, when terminated into either 600 or 900 ohms is:

Frequency Group	50 mA Line Current	70 mA Line Current	100 mA Line Current
Low Group (697-941)	-5.7 +/-1 dBm	-7.3 +/-1 dBm	-8.5 +/-1 dBm
High Group (1209-1633)	-3.2 +/-1 dBm	-4.8 +/-1 dBm	-6.0 +/-1 dBm



Notes:

1. Initial Transmission of RCC.

2. Initiator detects uncorrectable error in RCC and sends Retransmit RCC Request in lieu of Failed Call.

3. Responder receives retransmit request, retransmits RCC and waits for Crypto Sync.

4. Initiator receives RCC correctly and resumes Full Duplex sequence by decoding RCC and transmitting Crypto Sync.

Figure 2-18. Full Duplex Retransmit Sequence Initiator Request for RCC (V.26 or V.32 Mode)

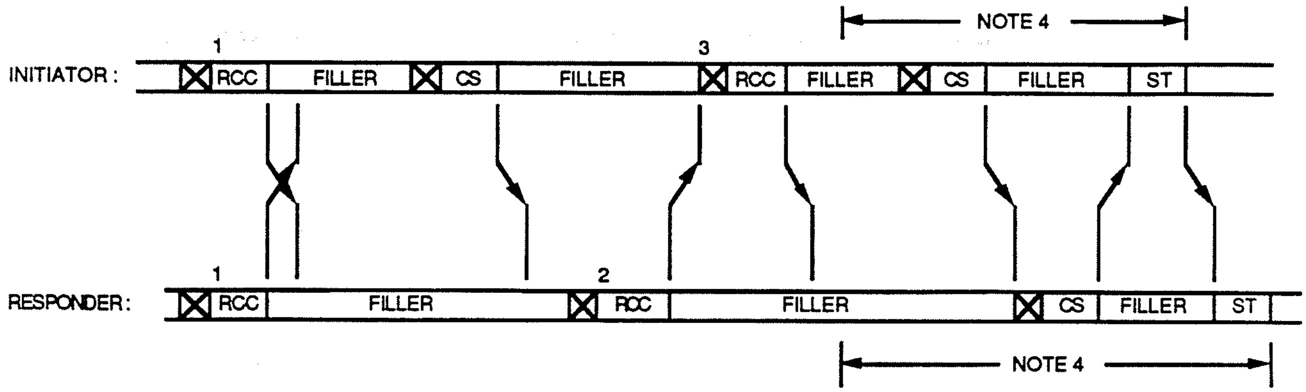
Similarly, retraining for 4800 or 9600 bps shall begin in exactly the same way as initial training for a 4800 or 9600 bps half duplex call. This shall continue through the initiator's transmission of P32L and SOM as shown in Figure 2-66. At this point the signaling skips the TC and RCC exchanges and proceeds directly to initial crypto sync. This shall be identical to the crypto sync used for initial call setup into a 4800 or 9600 bps half duplex call except that the longer P32L preamble is used by the responder prior to its CS message since this is the first transmission by the responder of the "V.32" preamble.

2.2.4 AUTOVON/DSN Network Operation

The STU-III terminals are required to provide a direct subscriber connection to the AUTOVON/DSN network in at least one configuration. It has been assumed that the STU-III will accommodate a 4-wire (separate transmit and receive pair) interface with typical DC signaling and supervision. In addition, all 2-wire STU-III terminals shall be capable of detecting an AUTOVON preemption and alerting the user as described in Section 2.2.4.1 below. The AUTOVON/DSN networks allow for both routine calling and four levels of precedence calling and preemption. Additional details concerning these networks are described in DCA Circular 370-V175-6. The primary signaling impacts to the STU-III using the 4-wire interface are in two areas: the DTMF signaling and preemption operation. Each of these is addressed in Section 2.2.4.2 below. This section does not attempt to define all of the electrical interfaces necessary to support an AUTOVON/DSN interface; rather it defines the additional signaling required to permit operation beyond the normal on/off hook and ring signaling and supervision. Terminal-to-terminal signaling for the 4-wire AUTOVON will be the same as for 2-wire signaling.

2.2.4.1 AUTOVON 2-Wire Interface Signaling

The STU-III, while operating in a secure mode, shall detect the AUTOVON preempt tone pair defined in DCA Circular 370-V175-6 within 500 msec of onset. The tone pair is 440 + 620 Hz, introduced at a composite level of -15 dBm,



Notes:

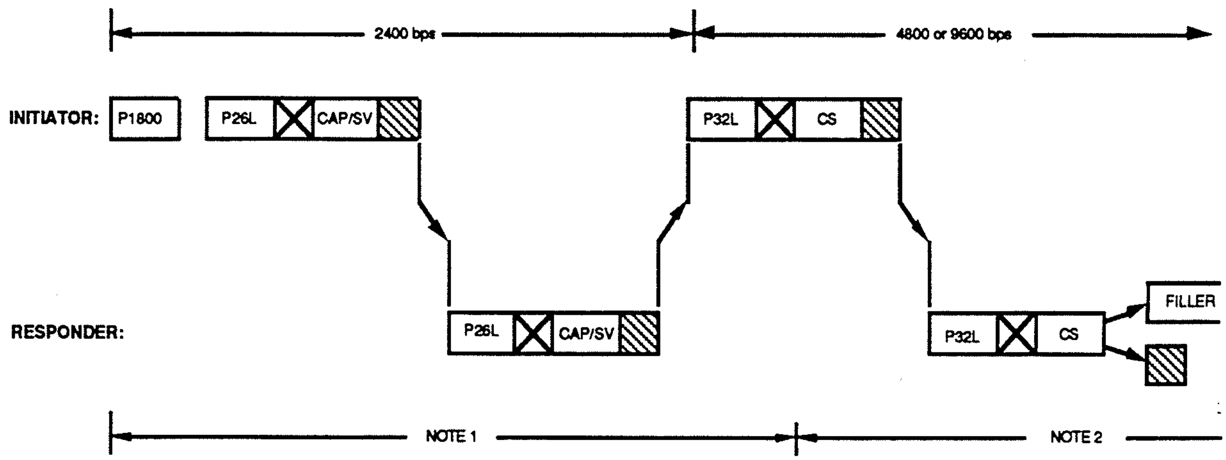
1. Initial Transmission of RCC.

2. Responder detects uncorrectable error in RCC, discards received Crypto Sync, and sends Retransmit RCC Request in lieu of Failed Call.

3. Initiator receives retransmit request, backs up to the transmit RCC state, transmits RCC and repeats the initial Crypto Sync.

4. Initial Sync Signaling.

Figure 2-19. Full Duplex Retransmit Sequence Responder Request for RCC (V.26 or V.32 Mode)



Notes:

1. Signaling as defined in Figure 2-62.

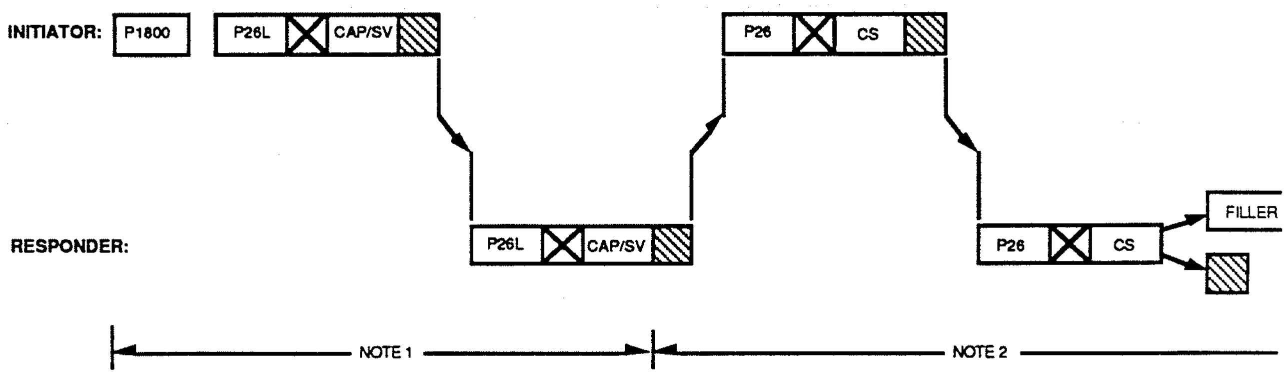
2. Signaling as defined in Figure 2-63, except P32L as shown for the first transmission in the V.32 mode.

Figure 2-66. Half Duplex 4800 or 9600 bps Retrain Signaling

Table 2-2. Timeouts for Terminals Implementing Full Duplex Retransmission Protocol

The appropriate terminal, as indicated in column A, shall set a timer during selected points in the call set-up as indicated in B. The timer setting is defined in C. If the timeout is exceeded before the expected message in D is detected, the terminal shall enter the signaling sequence in E. This table replaces Table 2-1 for terminals implementing the retransmission protocol. When the timeouts differ for the 2400 bps and V.32 modes, the timer value shown in parentheses applies to the V.32 mode.

A	B	C	D	E
Terminal Setting Timer	**Message Transmitted Starts Timer**	**Timer Value**	**Expected Response**	**Response to Timeout**
Initiator	Start of First 2100 Hz ESCD	3.3 ± .7 sec	P1800	Revert to analog call. Prompt user to abort call
Responder (2400 bps mode only)	Final Bit of SCR1	2.5 ± .6 sec (N/A)	2100 Hz	Revert to analog call. Prompt user to abort call
Responder (2400 bps mode only)	Start of P1800	20 ± 2 sec (N/A)	Valid CAP/SV	Failed Call
Initiator	Final Bit of CAP/SV	2.5 ± .6 sec	SOM of CAP/SV	Retransmit CAP/SV or Failed Call, per Figure 2-8
Either Terminal	Final Bit of TC	2.5 ± .6 sec	SOM of TC	Retransmit TC or Failed Call, per Figure 2-9
Either Terminal	Final Bit of RCC	5.0 ± .6 sec (5.8 ± .6 sec)	SOM of RCC	Retransmit RCC or Failed Call, per Figure 2-11
Initiator	Final Bit of initial CS	5.0 ± .6 sec (5.8 ± .6 sec)	SOM of CS	Retransmit CS or Failed Call, per Figure 2-12
Initiator	Final Bit of retry of initial CS	5.0 ± .6 sec (5.8 ± .6 sec)	SOM of CS	Retransmit CS or Failed Call, per Figure 2-12
Responder	Final Bit of RCC	10.0 ± .6 sec	SOM of CS	Failed Call
Either Terminal (Optional timeout for secure voice mode only)	Final bit of Start	2.5 ± .6 sec	Start	Initiate Crypto Resync or Failed Call
Leader	Final bit of CS mode change	2.5 ± .6 sec	ESC sequence (any)	Repeat CS mode change or Failed Call



Notes:

1. Signaling as defined in Figure 2-44.

2. Signaling as defined in Figure 2-48.

Figure 2-65. Half Duplex 2400 bps Retrain Signaling

Initial Synchronization. The initial synchronization immediately follows the Variable Exchange as part of the secure call set-up. The STU-III may initially enter only one of two modes: secure voice or secure data. The processing for initial synchronization is depicted in Figure 2-20.

The initiator will send a Start of Message (SOM), the CS message (with an MID indicating either the secure voice or the secure data mode) and Filler. The signaling for this phase is compelled such that the initiator will continue to transmit Filler until it receives the CS message from the other end or times out. The responder, upon completion of the Variable Exchange, waits for the CS message, and then proceeds to transmit its CS message followed by Filler. Figures 2-21 and 2-22 are timelines for the initial voice and data mode crypto synchronization, respectively.

As an option, the STU-III may provide the capability to retry initial synchronization. This option may be implemented by itself or in conjunction with the call setup message retransmission protocol defined earlier. To retry initial sync the initiator shall retransmit the initial CS message preceded by ESC. With the option implemented, the retry shall be transmitted in place of the Failed Call that would otherwise be sent after a timeout or receipt of a CS which fails the transmission validity checks that may have been imposed by the terminal. When implementing the option the initiator shall allow three retries of the initial sync before failing the call. When the responder implements this option it shall continue transmitting Filler until a valid initial sync is received from the initiator. With this option implemented the responder shall transmit Failed Call only after the CS timeout expires. The initial sync retry process is depicted in Figure 2-20, while an initial sync retry timeline is depicted in Figure 2-23.

The default situation for any mode conflicts is to go to secure voice operation. If the initiator sends the CS (Data) message and the Responder cannot support the mode, the Responder will transmit a CS (Voice) message, after which both

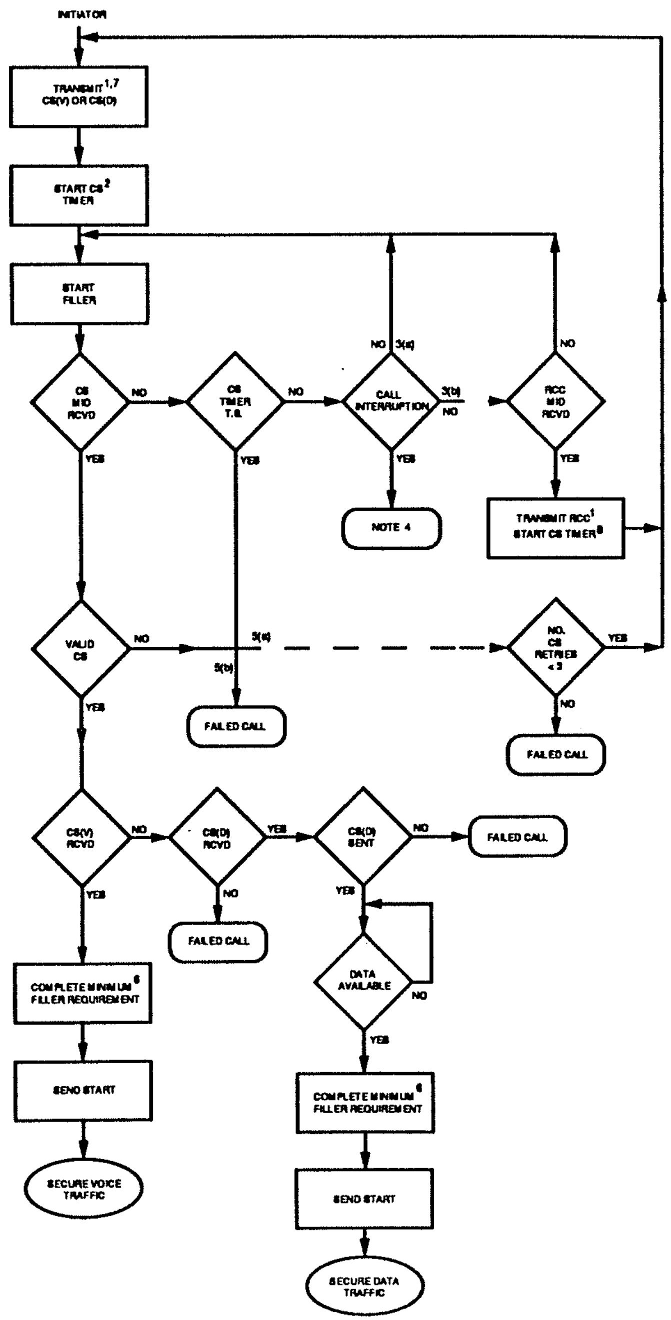
The retrain request is transmitted by the leader as shown in Figure 2-64. Upon receiving the Retrain Request the follower shall transmit the Retrain NACK if it is not willing to retrain. In this case, or if the initiator does not receive the Retrain ACK, the initiator shall continue in the same transmission format.

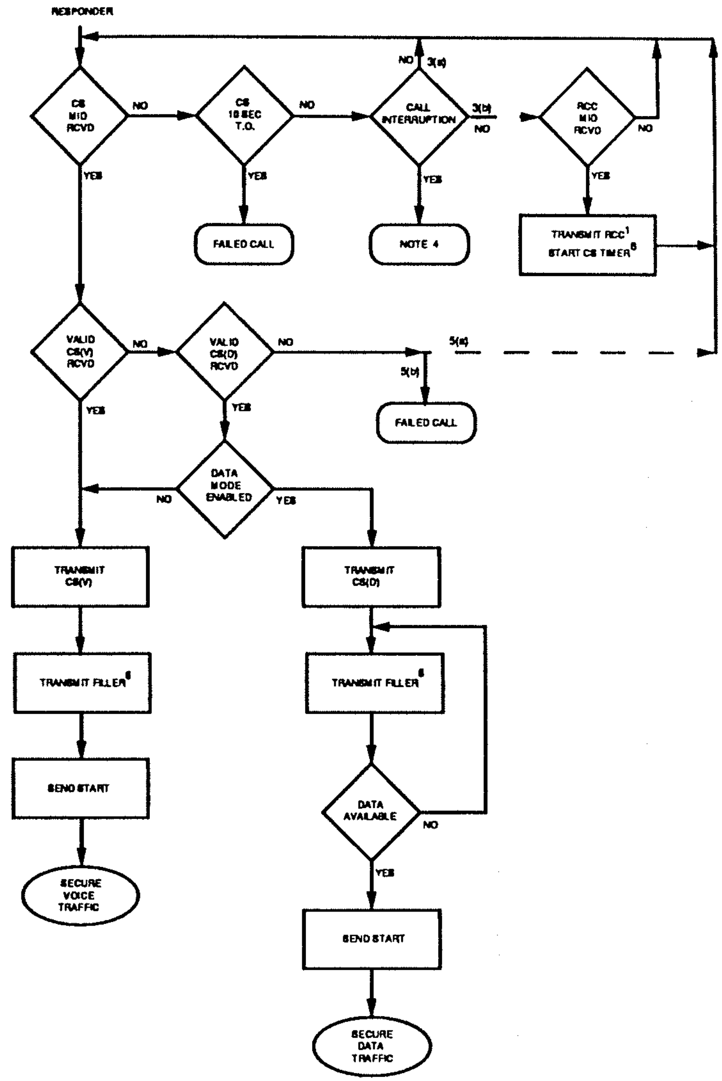
If the retrain request is accepted the follower shall transmit a Retrain ACK message followed by EOM, drop carrier, assume the role of responder, and prepare to respond to the retrain sequence transmitted by the leader.

Upon receiving the Retrain ACK from the follower, the leader shall initiate a retrain sequence into the same half duplex mode that was in use when the retrain request was transmitted, into an alternate half duplex mode, or into a full duplex mode. The half duplex retrain is initiated by the P1800 signal, while the full duplex retrain is initiated by the ESCD signal as described earlier. At the start of the P1800 or ESCD signal, the leader shall assume the role of initiator. It shall follow all rules for the initiator in such a way that the identification of initiator prior to the retrain shall have no further bearing on signaling.

2.2.3.2.6 Half Duplex Retrain Signaling Half duplex retraining shall be performed in accordance with the signaling described in this paragraph and in Figures 2-65 and 2-66. However, the leader/initiator in a retrain sequence shall initiate half duplex retraining only into one of those modes which the responder has indicated as available in the CAP/SV message most recently transmitted.

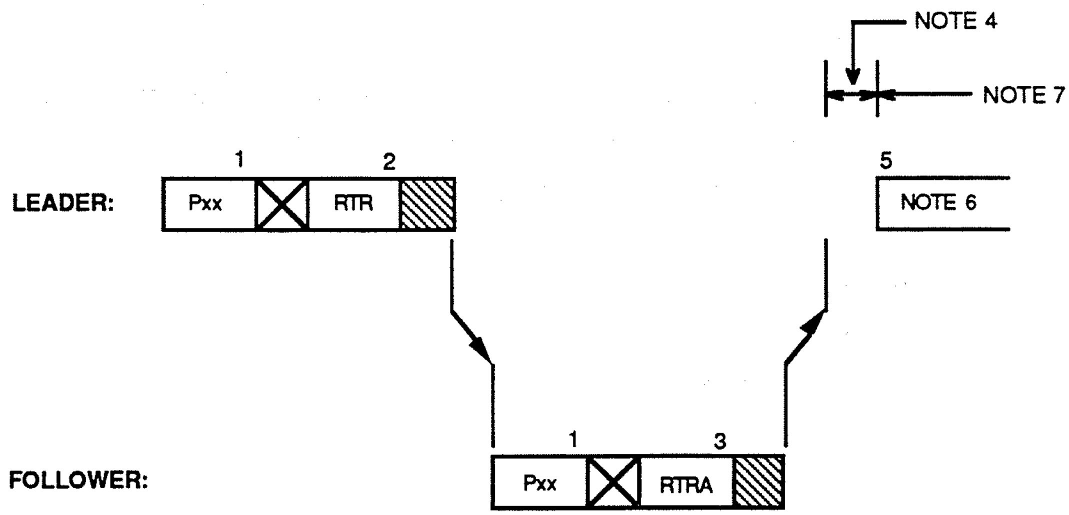
The retrain signaling for 2400 bps shall begin in exactly the same way as initial training for a 2400 bps half duplex call. As shown in Figure 2-65, the retraining and initial training are identical up through the transmission of CAP/SV by the responder. At the end of responder's CAP/SV the signaling skips the transmission of TC and RCC and proceeds directly to initial crypto sync. This part of the signaling shall be identical to the crypto sync signaling specified for a half duplex 2400 bps call following the exchange of TC and RCC.





Notes:
1. Terminals with retransmission protocol are subject to the transmit delay requirement of Section 2.2.1.3.1.7.
2. Per Table 2-1 or 2-2.
3(a). Path taken by terminals without retransmission protocol.
3(b). Path taken by terminals with retransmission protocol.
4. Process Abort, Failed Call or Release, as appropriate.
5(a). Path taken by terminals with CS retry capability.
5(b). Path taken by terminals without CS retry capability.
6. Transmission of Filler prior to Start must meet the minimum block requirements established for the mode and data rate in process.
7. On a CS retry, send ESC prior to SOM. ESC is not used on CS after RCC.
8. Per Table 2-2.
9. Test for validity shall only include examination of the CS MID field, and any BCH decoding tests used by the terminal.

Figure 2-20. Full Duplex Initial Sync Process Flow Diagram



Notes:

1. P26 or P32 depending on current format.
2. Retrain Request.
3. Retrain ACK. Alternatively the follower may refuse the retrain request by transmitting Retrain NACK.
4. Leader must wait a minimum of 75 ms and a maximum of 1 second after detecting drop of carrier before initiating retrain.
5. Leader assumes role of initiator.
6. ESCD for Full Duplex Retrain, P1800 for Half Duplex Retrain.
7. Retrain Signaling per Figures 2-60, 2-61, 2-65, or 2-66.

Figure 2-64. Half Duplex Retrain Request Signaling

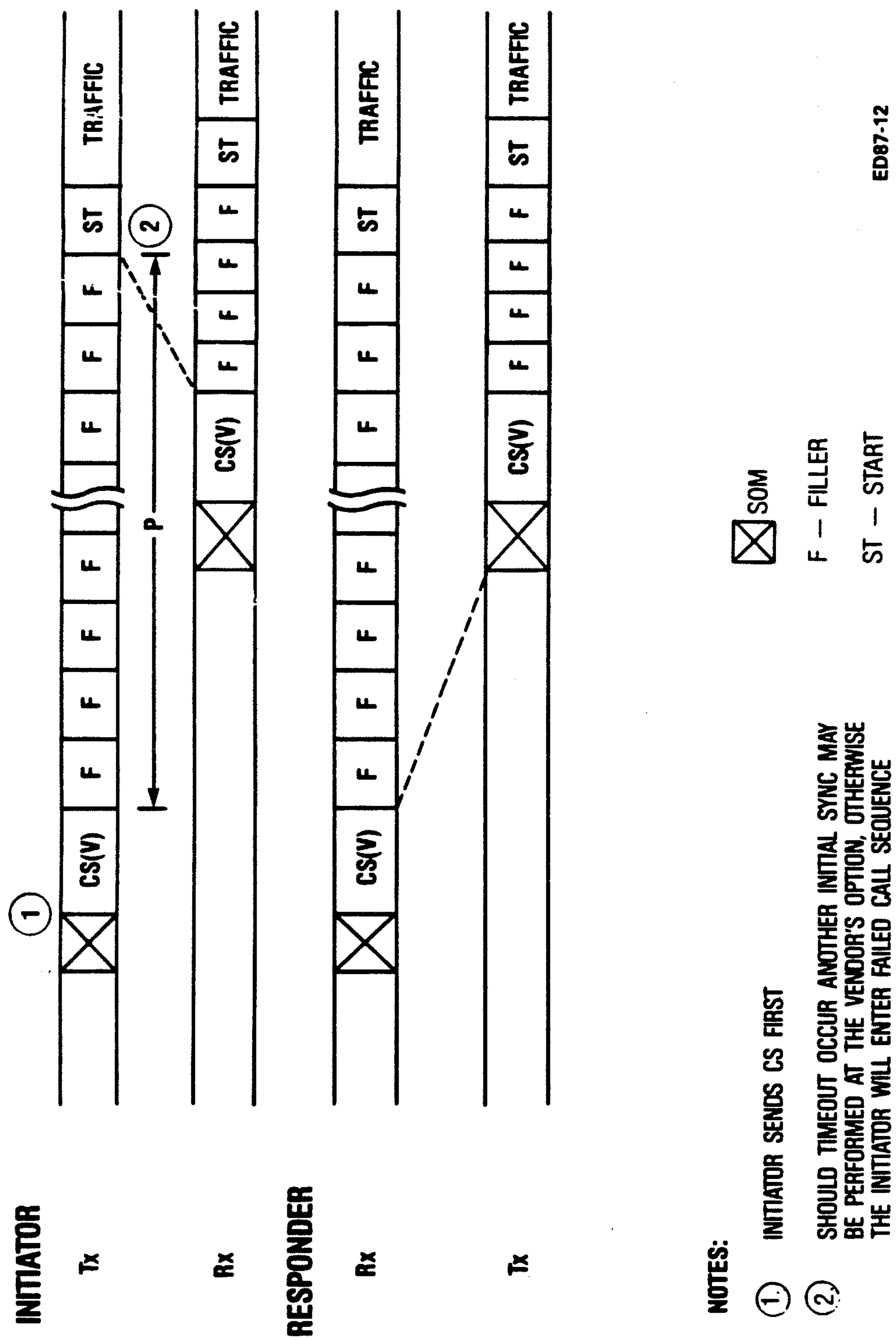


Figure 2-21. Initial Sync (Voice) Signaling Diagram

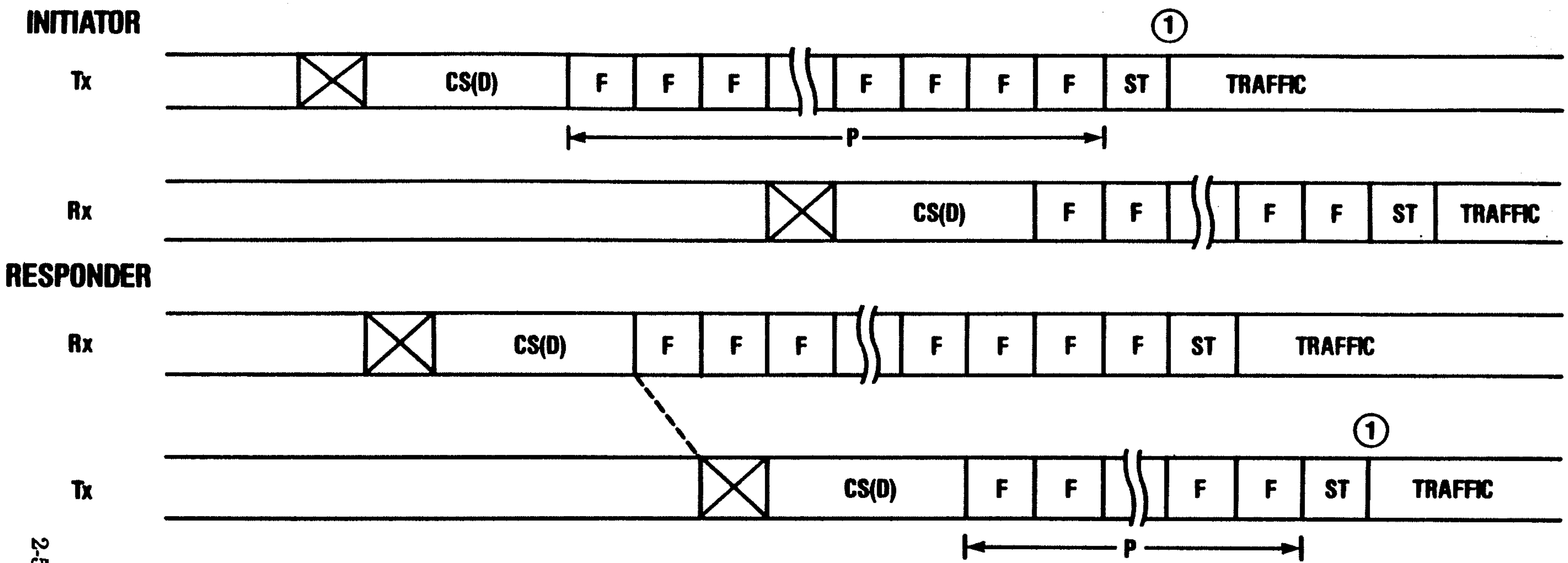
2.2.3.2.4 Signaling Modifications for Half Duplex "V.32" Transmission The format for data transmission in the half duplex "V.32" mode shall follow the approach defined for full duplex V.32 transmission. Thus, at 4800 bps each message dibit shall be transmitted in a single baud. At 9600 bps, all signaling messages shall be expanded with the message rate reducing dibit D_R = 01. The rate reducing dibit shall be applied in the same way it is applied in full duplex. Thus, the expansion shall be performed on all signaling messages except Filler transmitted between Crypto Sync and Start.

Requirements for the amount of Filler between CS and Start shall be identical to the requirement defined for the full duplex system.

Even though the rate reducing dibit used at 9600 bps has the effect of reducing the effective transmission rate to 4800 bps for signaling messages, the transmission mode in effect is defined as 9600 bps, and accordingly, the R2, R3 and E messages and the B1 training sequence shall indicate the 9600 bps rate.

Trellis coding may be used at 9600 bps. If used, it shall be indicated in the P32/P32L preamble to inform the remote terminal that subsequent transmissions will be sent with trellis coding. The trellis coding option shall be used only if both terminals have indicated in the CAP/SV that the half duplex trellis coding capability is available. When used, trellis coding shall be applied only to the B1 sequence, Filler between CS and Start, and to the secure traffic.

2.2.3.2.5 Half Duplex Retrain Request STU-IIIs offering either the 4800 or 9600 bps half duplex capability shall provide the capability to retrain the modem without repeating the entire exchange of call setup messages. The Retrain Request Message used as shown in Figure 2-64 shall be used to request retraining. This request shall not be made, however, until the terminal has transmitted its own initial CS and received the initial CS from the remote terminal. The retrain request may be made immediately after the initial CS exchange or later during traffic.



NOTES:

$p \geq 4$ FRAMES OF FILLER

(1) FIRST BIT OF TRAFFIC MARKED BY HAVING

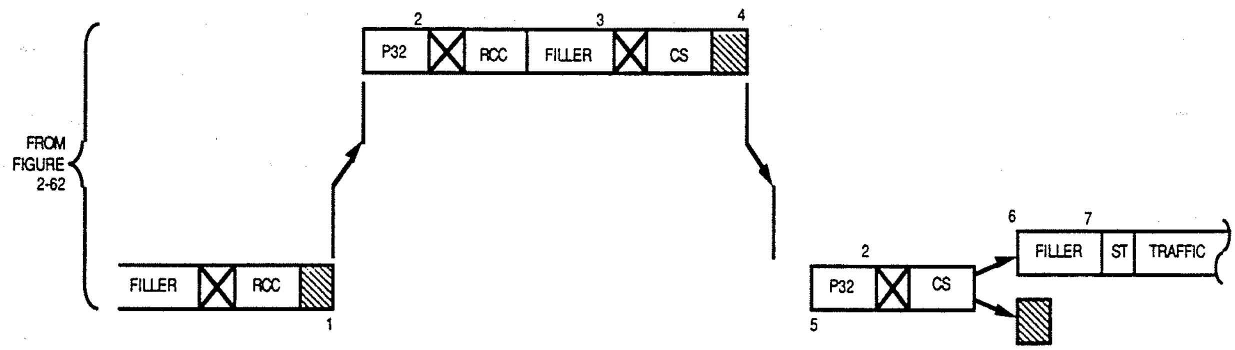
a) SENT CS(D) AND WAITED AT LEAST 4 FRAMES OF FILLER

AND b) RECEIVED CS(D)

AND c) DATA AVAILABLE FOR TRANSMISSION

ED87-13

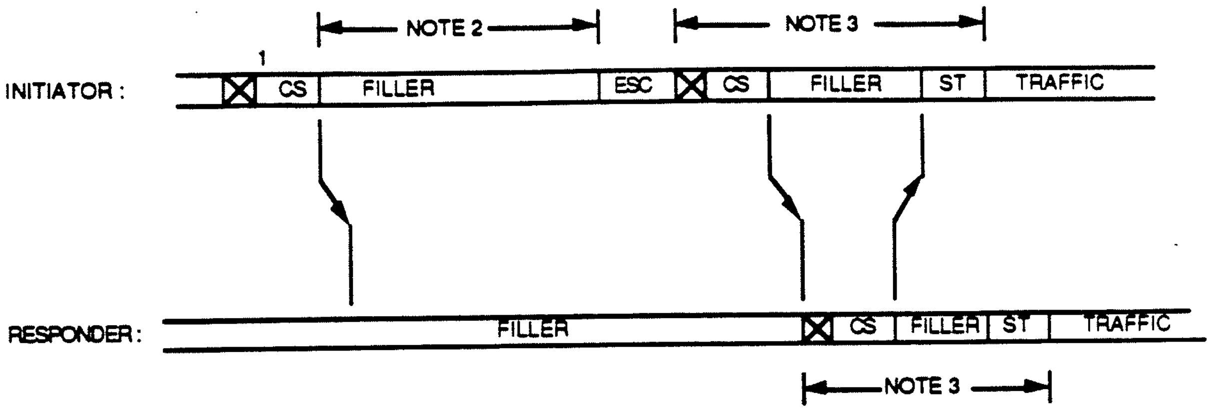
Figure 2-22. Initial Sync (Data) Signaling Diagram



Notes:

1. The responder shall start a 2.5 second timeout after transmitting EOM.
2. After the first transmission in the V.32 mode, the shorter P32 preamble is used.
3. The initiator transmits filler until the received RCC is decoded and processed and the Crypto Sync message is ready for transmission.
4. The initiator shall start a 6.5 second timeout after transmitting EOM.
5. The responder waits until the received RCC is decoded and processed and the Crypto Sync is ready for transmission.
6. CS is followed by either EOM, or Filler/SOM/traffic depending on the state of the responder's VOX (Voice Mode) or data availability (data mode).
7. For secure voice at 4800 bps 9 frames of filler shall be transmitted. For secure data at 4800 bps, 9 or more frames of filler shall be transmitted. For secure voice at 9600 bps, 19 frames of filler shall be transmitted. For secure data at 9600 bps, 19 or more frames of filler shall be transmitted.

Figure 2-63. Half Duplex Alternate Mode Signaling Diagram HDX V.32 Mode Selected (Exchange of RCC and CS)



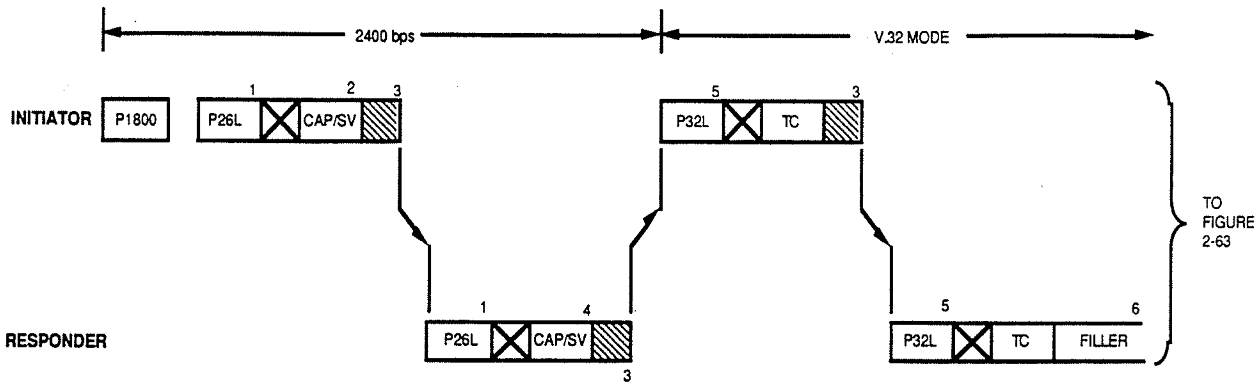
Notes:

1. Initial Transmission of Crypto Sync.

2. Initiator starts 5 second timeout at completion of CS. When timeout expires initiator retransmits CS preceded by ESC.

3. Initial Sync Signaling per Figure 2-21 or 2-22.

Figure 2-23. Initial Sync (with Retry) Signaling Diagram



Notes:

1. P26L is the P1800/SCRl preamble with 1024 bits of SCRl.

2. The initiator's CAP/SV contains the HDX Message A offering the V.32 format.

3. The transmitting terminal shall start a 2.5 ± .6 second timeout after transmitting EOM.

4. The responder's CAP/SV contains the HDX Message B accepting the V.32 format.

5. The P32L preamble is used on the first transmission of P32 by both the initiator and responder.

6. The responder transmits Filler until RCC is ready for transmission.

Figure 2-62. Half Duplex Alternate Mode Signaling Diagram HDX V.32 Mode Selected (Exchange of CAP/SV and TC) terminals will enter the secure voice mode. Alternatively, if the Responder has the data mode enabled but receives a CS (Voice) message, it will transmit a CS (Voice) message and enter the secure voice mode.

If the secure voice mode is selected by the initiator, each terminal must receive the far-end CS (voice) message. The initiator shall transmit Filler (minimum of four frames) until the CS (voice) is received from the responder. The initiator may then transmit Start and enter the secure mode (Transmit). The responder, upon receipt of CS (voice) from the initiator, shall transmit CS (voice) followed by a minimum of four frames of Filler, and then Start to enter the secure voice mode.

If the secure data mode is selected, each terminal will delay the start of secure traffic, continuing to send Filler (a minimum of four frames) until data is available for transmission. The STU-III shall ensure that the first bit of available data is the first bit encrypted and the first bit transmitted in the secure data mode transmission. Each terminal will transmit a Start message immediately preceding the secure data traffic such that the secure mode (Receive) will be initiated upon receipt of the far-end terminal's Start message. It should be noted that either terminal may send Filler continuously (e.g., for operation of a simplex, one-way transmission data device being used over a full duplex secure link).

Resynchronization. There are several secure modes that the STU-III may support (e.g., secure voice, secure data, BERT Test, secure dial). As indicated above, the terminals will enter either the secure voice or data mode initially. Once the STU-IIIs are in a secure traffic mode, either or both of them may detect, or otherwise determine that an out-of-sync condition has occurred. Either terminal may initiate a resynchronization procedure (i.e., to the same mode or to a new mode).

Each terminal shall use the P32L preamble for its first transmission after a change into the V.32 half duplex mode. Subsequent transmissions in the same format shall use the shorter P32 preamble.

As with full duplex the initiator shall use the scrambler for the call mode modem and transmit the R2 message. Similarly, the responder shall use the scrambler for the answer mode modem and transmit the R3 message. In addition, the V.32 rules shall apply up to the end of the Bl sequence. At the transition from the Bl sequence to the SOM immediately following, the standard rules shall apply that are used for the 2400 bps interoperable mode.

2.2.3.2.3 <u>Half Duplex Call Setup for "V.32" Transmission</u> Call Setup in half duplex for all formats shall be initiated as described in Figure 2-44.

The initiator wishing to change from the 2400 bps format to the "V.32" half duplex format shall set the appropriate bits in the HDX Message A/B reserved bytes in the CAP/SV. These bits correspond in order, meaning and use to those defined for the two bytes of Message A and B in full duplex transmission. As with full duplex, the responder shall select a mode of transmission from one of those offered and indicate its selection by setting the appropriate bit in the HDX Message A/B reserved bytes in its CAP/SV.

If the responder accepts the offer to change to the "V.32" format, it shall send only the CAP/SV followed by EOM, as shown in Figure 2-62, and wait for the next transmission from the initiator. If the responder does not accept the offer it shall either send CAP/SV with the 2400 HDX bit set in Byte one of the A/B message or send CAP/SV with all zeroes in the Message A/B field and continue with the standard half duplex 2400 bps call setup sequence. When the offer is accepted, the initiator shall send TC preceded by the P32L preamble. The responder shall continue by sending P32L, TC, filler and RCC. As shown in Figure 2-63 the initiator shall then send the shorter P32 preamble, RCC, filler, the CS message and EOM. As with 2400 bps signaling the responder may then respond with either CS/EOM or CS/Filler/ST and traffic depending on its readiness to send traffic.

The terminal that starts the resynchronization assumes the leader role and transmits ESC/SOM, the appropriate Crypto Sync message and Filler. There are unique MIDs that identify the mode requested. The signaling for resynchronization or a mode change (not including one-way mode changes, such as secure dial) is compelled. Thus, the leader will continue to send Filler (a minimum of four frames) until it receives a CS message from the far end. If the modes agree, the leader continues into the secure traffic mode selected. As in the case of the initial sync, the STU-IIIs will default to the secure voice mode if a conflict results. If the leader times out before receiving a CS message from the far end, it may retransmit ESC/SOM and the CS message. A maximum number of attempts for transmission of the CS message after a timeout (including zero retries) may be established at the vendor's option.

The terminal that detects the ESC/SOM assumes the role of follower. As in the case of the initial sync operation, the follower will not transmit a CS message until it receives a CS message. If it can support the mode indicated by the MID associated with the CS message, it will send ESC/SOM, the appropriate CS message, at least four frames of Filler (longer if the particular mode requires) and Start. It then can enter secure traffic. If the terminal cannot support the mode (e.g., if the data mode is not enabled, the terminal cannot support secure data), the follower will transmit a CS (Voice) message and revert to the secure voice mode. If the terminal does not recognize the MID, it will transition to Failed Call (Section 2.2.1.6).

If the mode received by the leader in the CS message differs from that in the CS message it transmitted, it will revert to secure voice. Typically, the far-end terminal will send a CS (Voice) message in response if the modes conflict. Figure 2-24 depicts the processing for the full duplex resynchronization processing. The timelines depicting the resynchronization signaling for the voice and data modes, respectively, are provided in Figures 2-25 and 2-26. The timelines for transitioning from the voice to data mode, and the data to voice mode are provided in Figures 2-27 and 2-28, respectively.

2.2.3.2 Half Duplex Operation Using Rec. V.32 Modulation Format

2.2.3.2.1 Half Duplex Modulation Formats The STU-III may provide half duplex modes of operation using the V.32 modulation format to transmit and receive data. With the exception that these shall be available in a half duplex mode, the modulation formats used for transmission of data shall be identical to those provided in full duplex. The preambles and training sequences are adapted from the full duplex format and are described below.

2.2.3.2.2 Half Duplex Preambles for V.32 Transmission For half duplex transmission using the V.32 modulation format, the preamble shall be constructed of the same elements used by the V.32 modem prior to transmitting data. For the call mode modem this shall include the S, Complement of S, TRN, R2, E and Bl sequences described in Rec. V.32, paragraph 5.4.1. Similarly, the answer mode modem shall use the S, Complement of S, TRN, R3, E and B1 sequences described in Rec V.32 paragraph 5.4.2. These signal segments shall be identical to those described with 3 exceptions: (1) The S sequence shall be 768 symbols long to allow enough time for network echo suppressors to release, (2) TRN shall be limited to 424 symbols, and (3) R2 or R3 shall contain only 2 repetitions of the rate signal. The format of R2 or R3 and E shall be identical to that described for full duplex signaling, but in the half duplex preamble shall signify the mode of transmission to follow with the understanding that these apply to a half duplex mode. Thus, in the R2, R3 and E messages, the appropriate bits shall be set to indicate the data rate for the transmission to follow. If the rate is 9600 bps, the trellis coding bit may be set to indicate that trellis coding will be in effect. This preamble is denoted as P32 in the signaling diagrams contained in this section. Where P32L is indicated it shall be the same as P32 except that the TRN segment shall correspond exactly to the V.32 definition and shall contain 1280 symbols.

The signaling for a mode change to secure dial or to any one-way voice or data mode is not compelled. Thus the leader will send four frames of Filler, Start, and will begin to transmit the secure traffic indicated in the MID. If the follower cannot support the one-way mode selected by the leader, the follower will enter the Failed Call sequence.

The signaling has been designed to permit operation if both terminals attempt to resynchronize at the same time. In this situation, each terminal assumes a leader role. If the modes indicated in the CS messages differ, both terminals will enter the secure voice mode after receiving the far-end CS message. Figure 2-29 depicts the timeline for this situation. If the same mode is selected by both terminals, the desired mode will be entered as depicted in Figure 2-30.

2.2.1.5 Full Duplex Secure Traffic

The next phase in the call set-up between the STU-IIIs is secure traffic. The functions of the STU-III in this phase are to process:

- Secure Voice
- Secure Data (synchronous and asychronous)
- Secure Dialing
- Bit Error Rate Testing

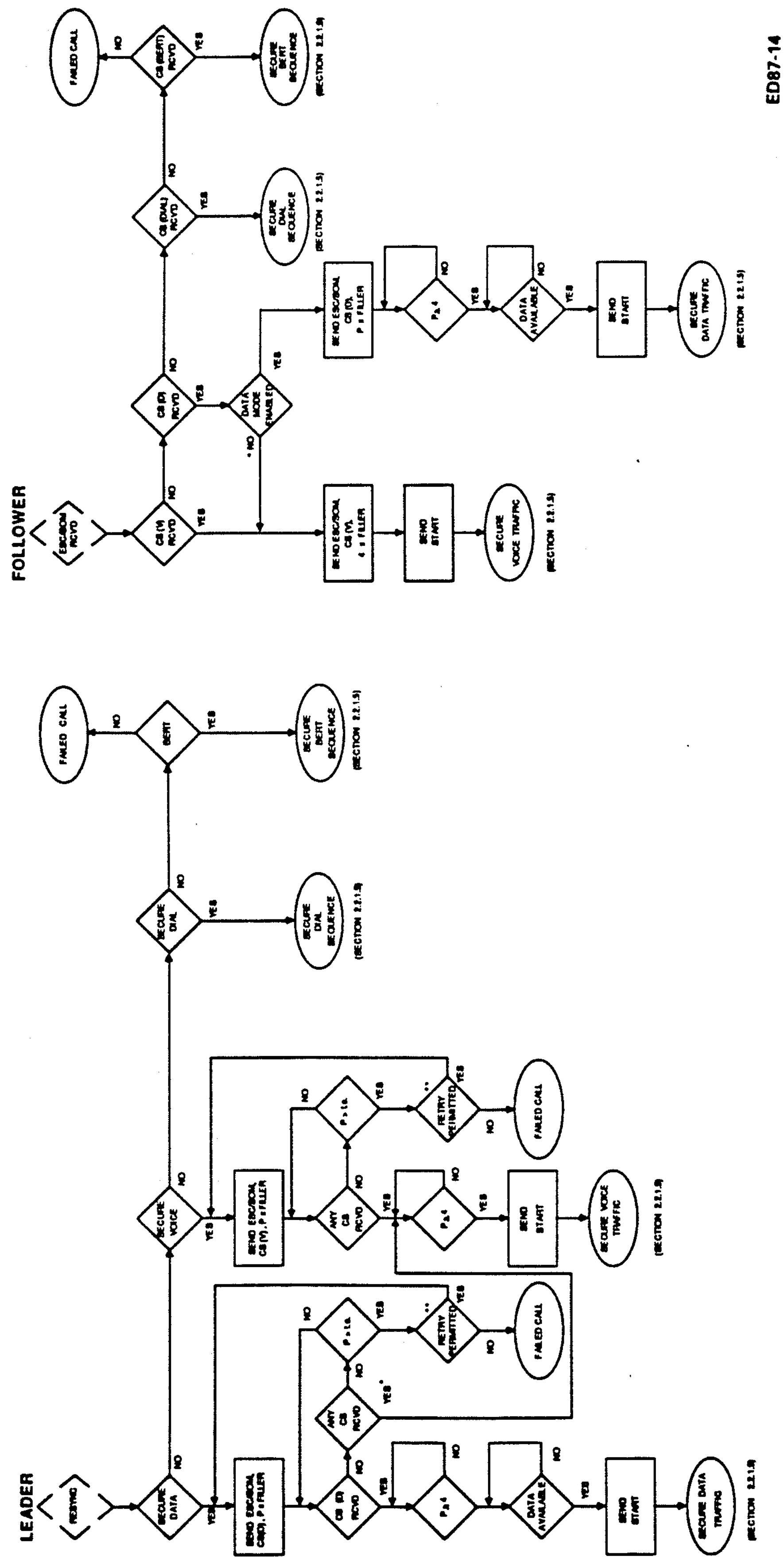
In addition to the normal secure processing, the STU-III shall monitor the secure traffic for Escape sequences, and shall disable secure traffic in the event of a hardware malfunction or user initiated interruption (e.g., activating a Non-Secure control, going on hook).

There are several other events which must be monitored during secure traffic. The flowchart in Figure 2-31 depicts the various functions or conditions for which the STU-III has to monitor including the user going on hook, removing the CIK, activating a Non-Secure control, changing modes (e.g., initiating secure dialing).

The signaling to retrain into 2400 bps is intended to be identical to that used for modem training when a call is initially established at 2400 bps. As shown in Figure 2-60, however, the ESCD shall always be used. The responder shall transmit the phase reversals in the P1800 signal if it wants to allow the initiator the option to retrain into a V.32 mode through the use of A/B signaling. If the responder wants to force the retrain to the standard 2400 bps it may transmit P1800 without the phase reversals.

Immediately following the completion of the SCR1 sequence, the initiator shall transmit SOM/CS/Filler following the rules for initial synchronization. The responder shall wait for the arrival of the initiator's SCR1/SOM transition before beginning transmission of the second SCR1 segment. Within 300 milliseconds after the arrival of the SCR1/SOM transition, the responder shall begin the transmission of 704 bits of the SCR1 sequence (GPA scrambler). This time window is specifically intended to allow, but not require, the responder to delay the beginning of SCR1 until after reception of the initiator's CS. Immediately following the transmission of the 704 bits of SCR1, the responder shall transmit SOM/CS, Filler, or a continuation of the SCR1 sequence. The SOM/CS sequence may be transmitted immediately after the 704 bits of SCR1 ifthe initiator's CS has been received and the responder's CS is ready for transmission. Otherwise, Filler or SCR1 shall be transmitted until the responder's CS is ready for transmission.

The signaling to retrain into the V.32 mode is intended to be identical to the modem training used for initial entry into the V.32 mode. As with the initial entry into the V.32 mode, the initiator shall transmit SOM/CS/Filler immediately following the B1 sequence. Rules for initial synchronization shall be followed. When the responder has completed transmission of the B1 sequence required by the V.32 protocol, it shall transmit Filler or a continuation of the B1 sequence until ready to transmit SOM/CS/Filler to complete the initial crypto sync exchange.

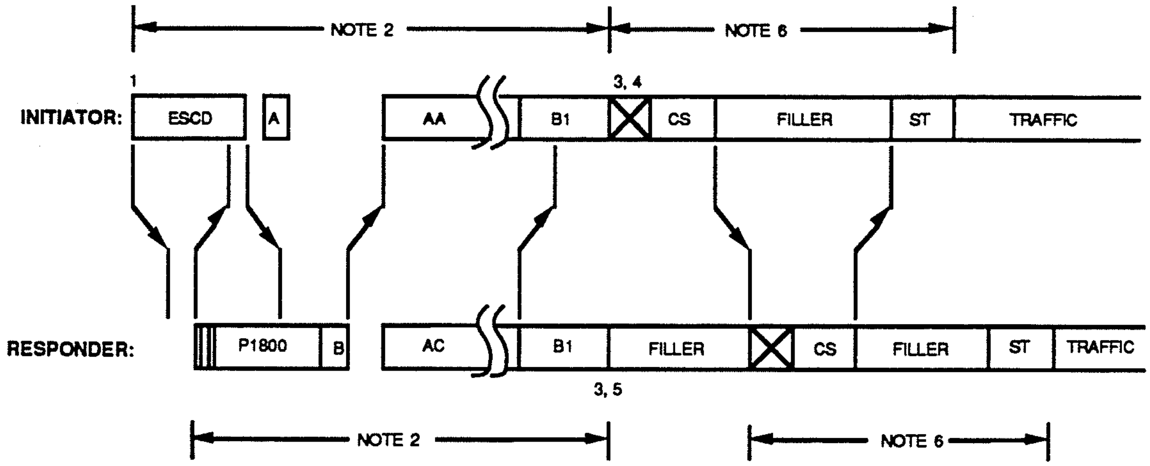


* REVERT TO SECURE VOICE MODE

** AT THE VENDOR'S OPTION, A MAXIMUM MAY BE SET, INCLUDING ZERO, FOR THE NUMBER OF TIMES A RETRY IS PERMITTED

t_0 = NOMINAL 2.5 SECONDS

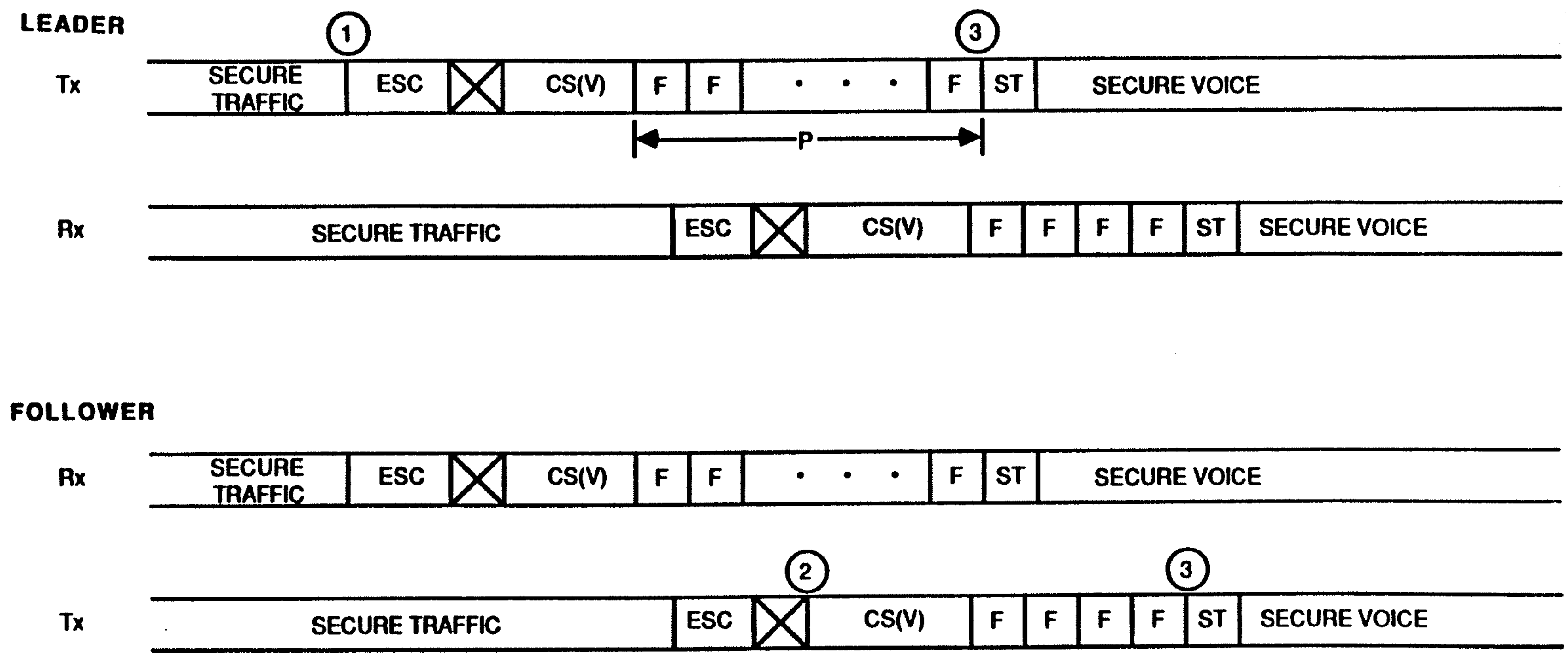
Figure 2-24. Full Duplex Resynchronization Process Flow Diagram



Notes:

1. Leader in Retrain Request Signaling assumes role of initiator.
2. Signaling in accordance with Figure 2-8.
3. At the completion of the B1 sequence, the rules of the FSVS-210 scrambler begin.
4. Initiator transmits SOM/CS immediately following the B1 segment.
5. At the completion of the B1 sequence required by V.32 the responder transits Filler per FSVS-210, or continues the B1 sequence per V.32 until SOM/CS is ready for transmission.
6. Initial Sync Signaling per Figure 2-21 or 2-22.

Figure 2-61. Full Duplex V.32 Retrain Signaling



NOTES:

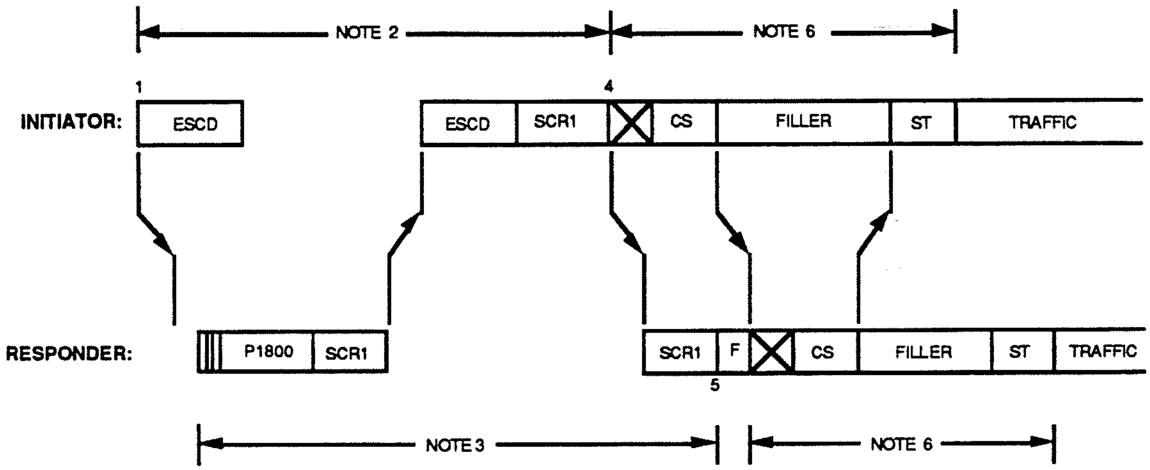
1 LEADER INITIATES MODE CHANGE

2 FOLLOWER DETERMINES MODE FROM CS MID

3 CS(V) RCVD FROM FAR END, AND P ≥ 4

ED87-15

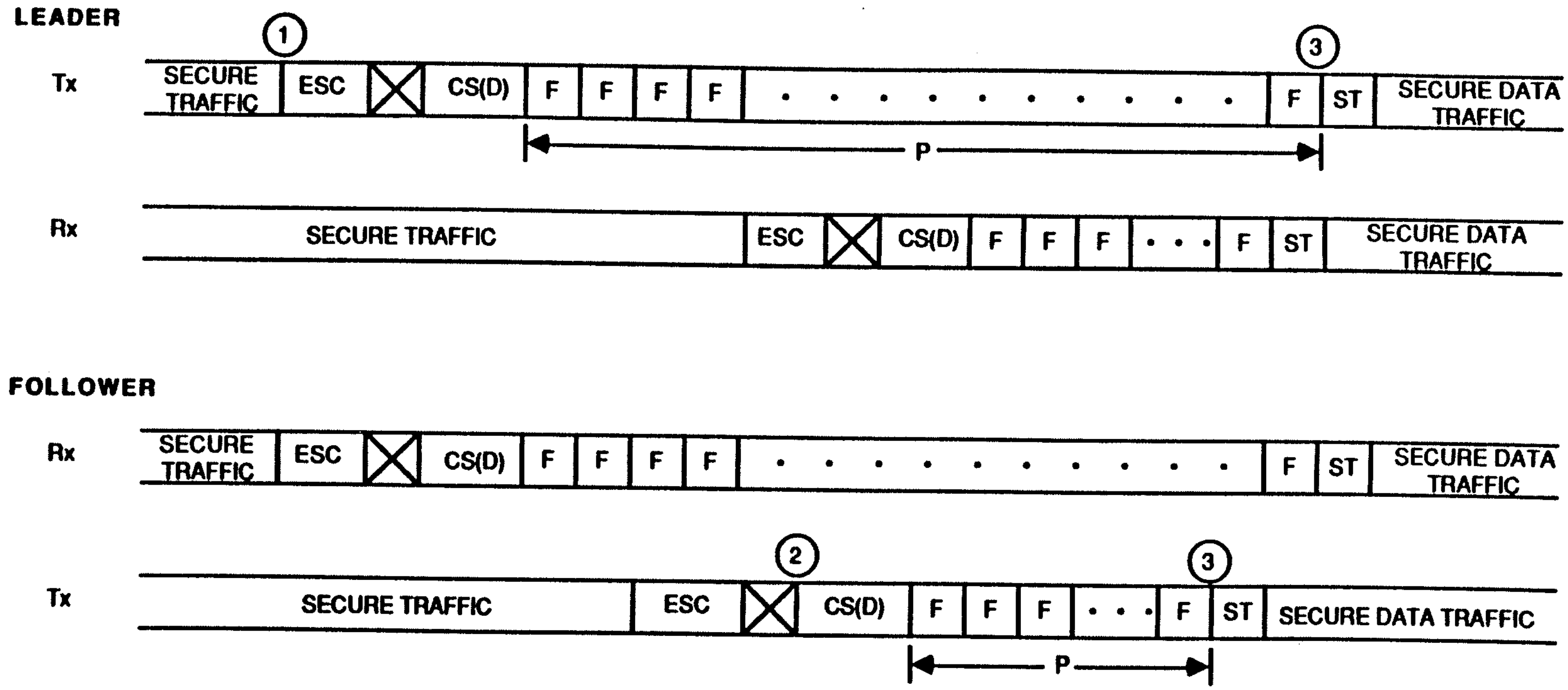
Figure 2-25. Resync Full Duplex Voice Mode (End-Around) Signaling Diagram



Notes:

1. Leader in Retrain Request Signaling assumes role of initiator.
2. Initiator Signaling per Figure 2-4, except ESCD required.
3. Responder Signaling per Figure 2-3 or 2-4.
4. Initiator transmits SOM/CS immediately following SCR1.
5. If not ready to transmit SOM/CS, the responder transmits Filler or continues SCR1 until ready to transmit SOM/CS.
6. Initial Sync Signaling per Figure 2-21 or 2-22.

Figure 2-60. Full Duplex 2400 bps Retrain Signaling



NOTES:

1. LEADER INITIATES MODE CHANGE
2. FOLLOWER DETERMINES MODE FROM CS MID
3. DATA AVAILABLE, CS(D) RCVD FROM FAR END, AND $P \geq 4$

ED87-16

Figure 2-26. Resync Full Duplex Data Mode (End-Around) Signaling Diagram to retrain. In this case or after a timeout of 2.5$\pm$.6 seconds without receiving an ESC followed by a drop in carrier the leader shall initiate a resynchronization following the rules described in Section 2.2.1.4.

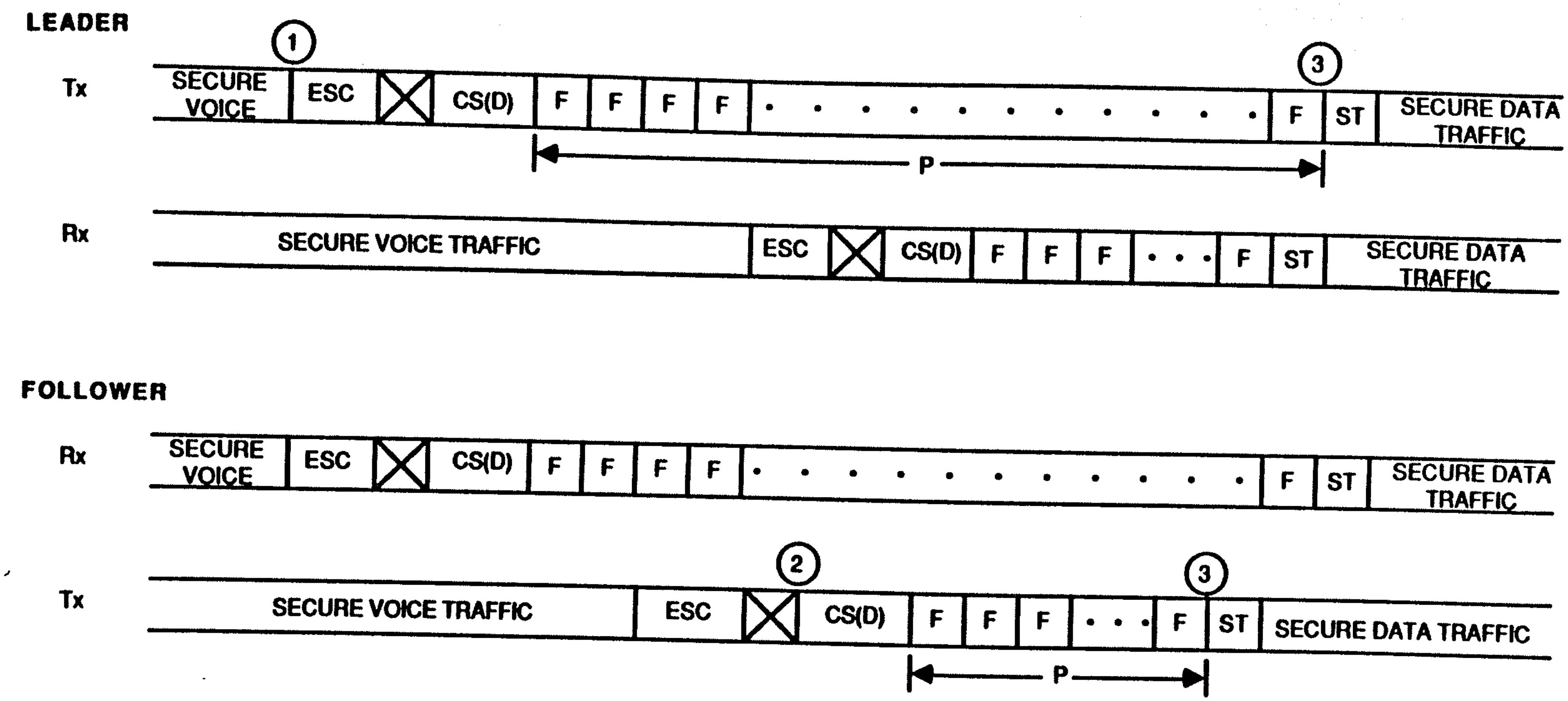
If the retrain request is accepted, the follower shall send ESC and drop carrier, assume the role of responder and prepare to respond to the retrain sequence transmitted by the leader.

Upon receiving an ESC from the follower followed by a drop in carrier indicating acceptance of the retrain request, the leader shall drop carrier, assume the role of initiator and proceed with the desired retraining sequence.

In the event of a glare condition where both terminals transmitted the Retrain Request message, the initiator's Retrain Request shall take precedence. After receiving the initiator's Retrain Request, the responder shall transmit ESC, drop carrier and continue with the retrain sequence as described above.

Following acceptance of the retrain request, the leader shall initiate a retrain sequence into the same full duplex mode that was in use when the retrain request was transmitted, into an alternate full duplex mode, or into a half duplex mode. The full duplex retrain is initiated by the ESCD signal while the half duplex retrain is initiated by P1800 as described later. At the start of the ESCD or P1800 signal the leader assumes the role of initiator. It shall follow all rules for the initiator in such a way that the identification of initiator prior to the retrain shall have no further bearing on signaling.

2.2.3.1.8 Full Duplex Retrain Signaling Full duplex retraining shall be performed in accordance with the signaling described in this paragraph and in Figures 2-60 and 2-61 for 2400 bps and V.32 retraining respectively. However, the leader/initiator in a retrain sequence shall initiate full duplex retraining only into one of those modes which the responder has indicated as available in the CAP/SV message most recently transmitted.

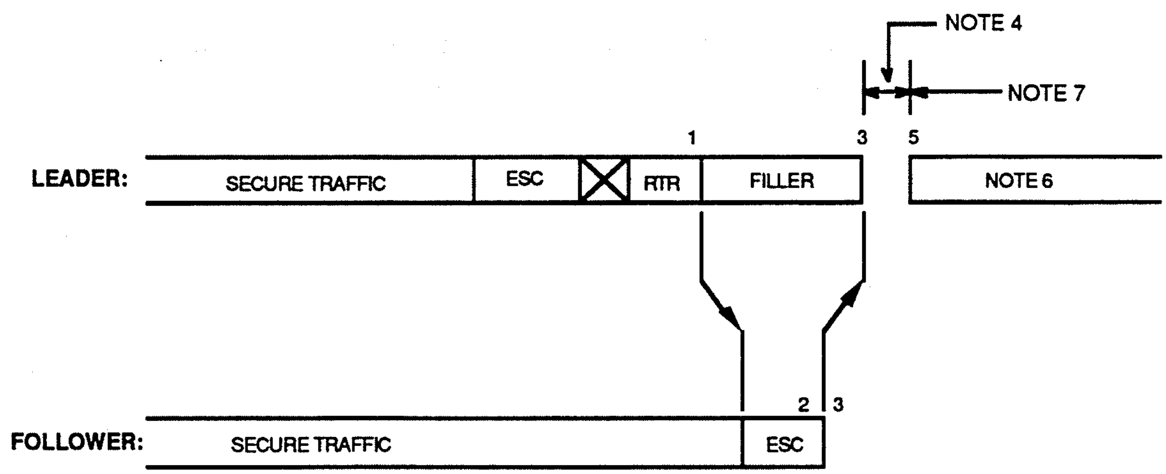


NOTES:

1. LEADER INITIATES MODE CHANGE
2. FOLLOWER DETERMINES MODE FROM CS MID
3. DATA AVAILABLE, CS(D) RCVD FROM FAR END, AND P ≥ 4

ED87-17

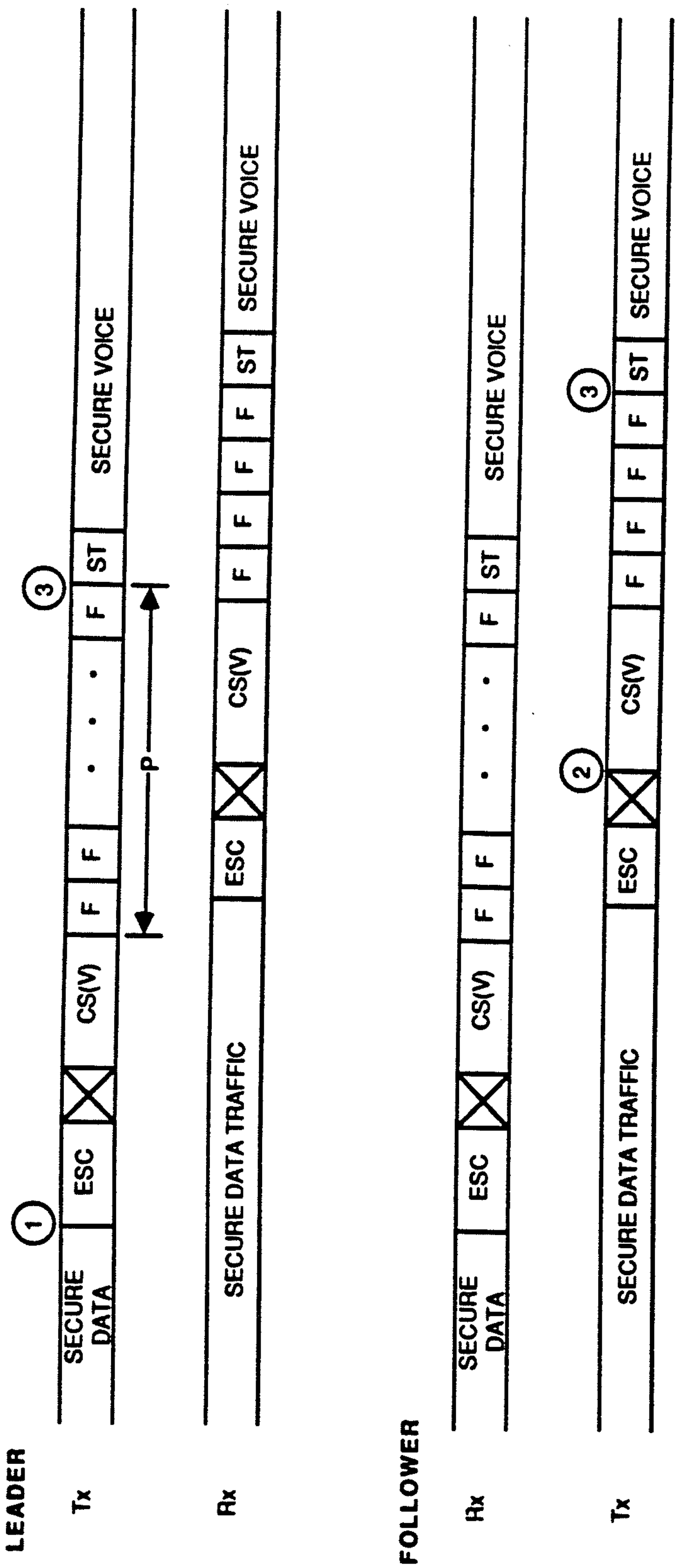
Figure 2-27. Full Duplex Mode Change (Voice-to-Data) Signaling Diagram



Notes:

1. Retrain Request Message
2. Follower may alternatively transmit ESC/Retrain NACK/Filler to refuse retrain request.
3. Terminals drop carrier
4. Leader must wait a minimum of 75ms and a maximum of 1 second after detecting drop of carrier before initiating retrain.
5. Leader assumes role of initiator
6. ESCD for Full Duplex Retrain, P1800 for Half Duplex Retrain
7. Retrain Signaling per Figures 2-60, 2-61, 2-65 or 2-66

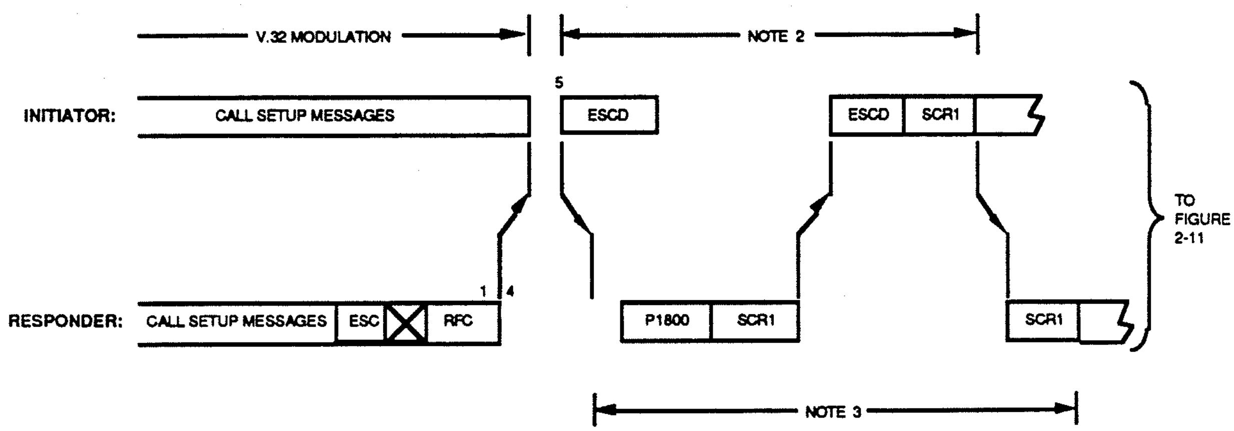
Figure 2-59. Full Duplex Retrain Request Signaling



NOTES:

1. LEADER INITIATES MODE CHANGE
2. FOLLOWER DETERMINES MODE FROM CS MID
3. CS(V) RCVD FROM FAR END, AND P ≥ 4

Figure 2-28. Full Duplex Mode Change (Data-to-Voice) Signaling Diagram



Notes:

1. Restart Failed Call Message.

2. Initiator Signaling per Figure 2-3.

3. Responder Signaling per Figure 2-3.

4. Responder Timeout starts here. If ESCD signaling not received within 10 seconds, responder shall complete a standard failed call sequence.

5. Initiator starts sending ESCD 2 second ± 200 ms after seeing responder's carrier drop.

Figure 2-58. Full Duplex Call Setup Restart at 2400 bps (Led by Responder)

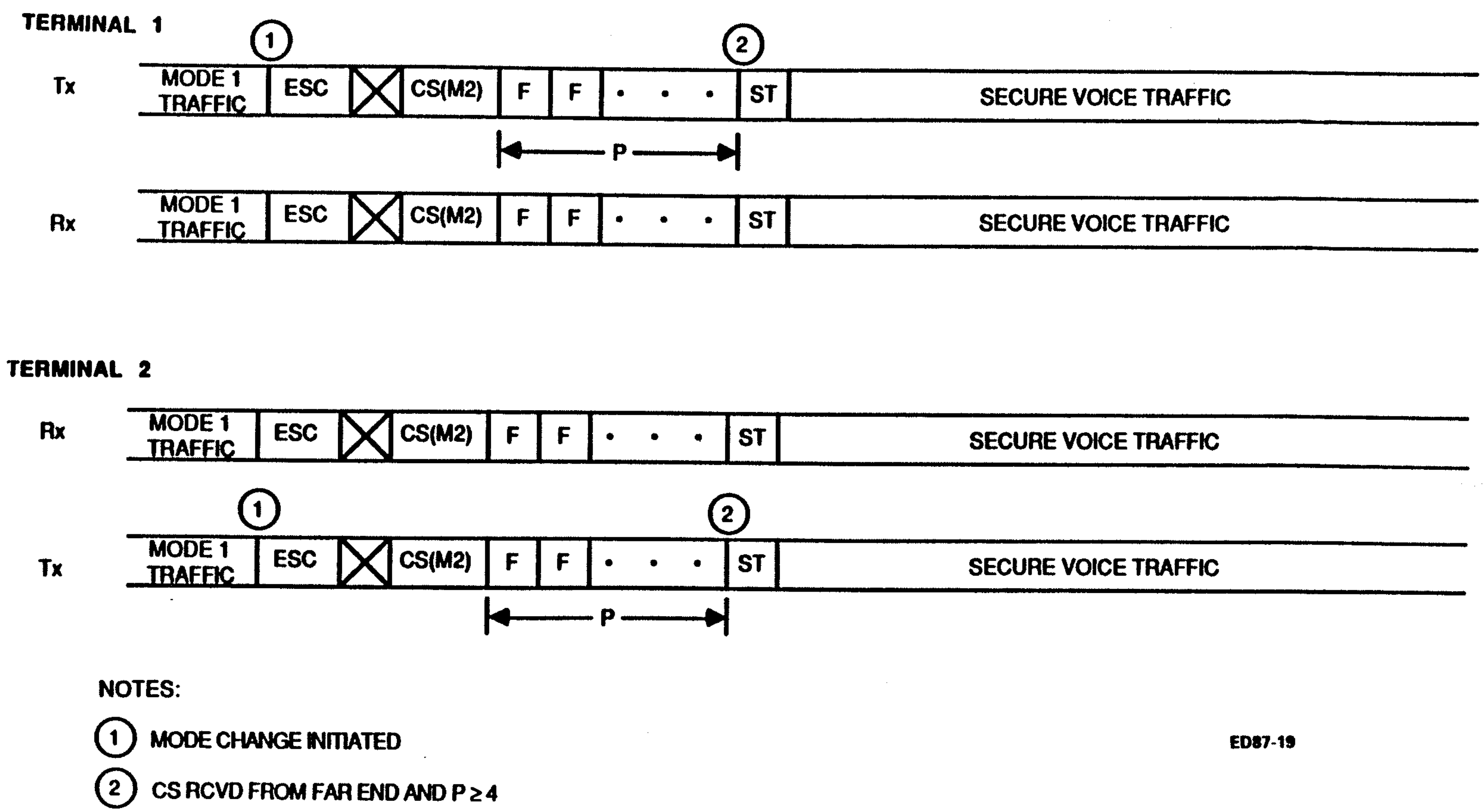
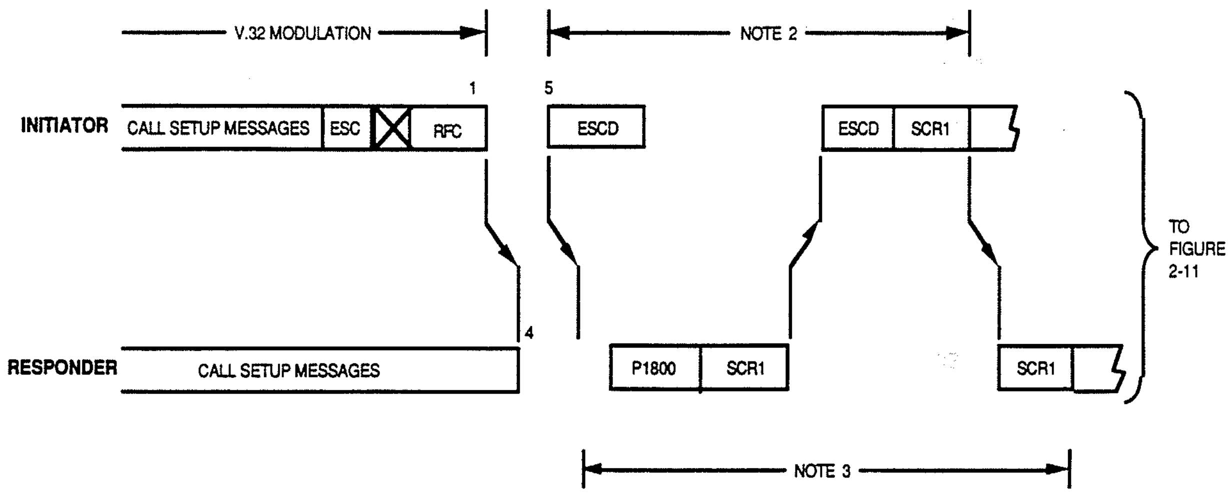


Figure 2-29. Full Duplex Mode Change – Different Mode (Simultaneous) Signaling Diagram



Notes:

1. Restart Failed Call Message.

2. Initiator Signaling per Figure 2-3.

3. Responder Signaling per Figure 2-3.

4. Responder Timeout starts here. If ESCD signaling not received within 10 seconds, responder shall complete a standard failed call sequence.

5. Initiator starts sending ESCD 2 seconds ± 200 ms after dropping carrier.

Figure 2-57. Full Duplex Call Setup Restart at 2400 bps (Led by Initiator)

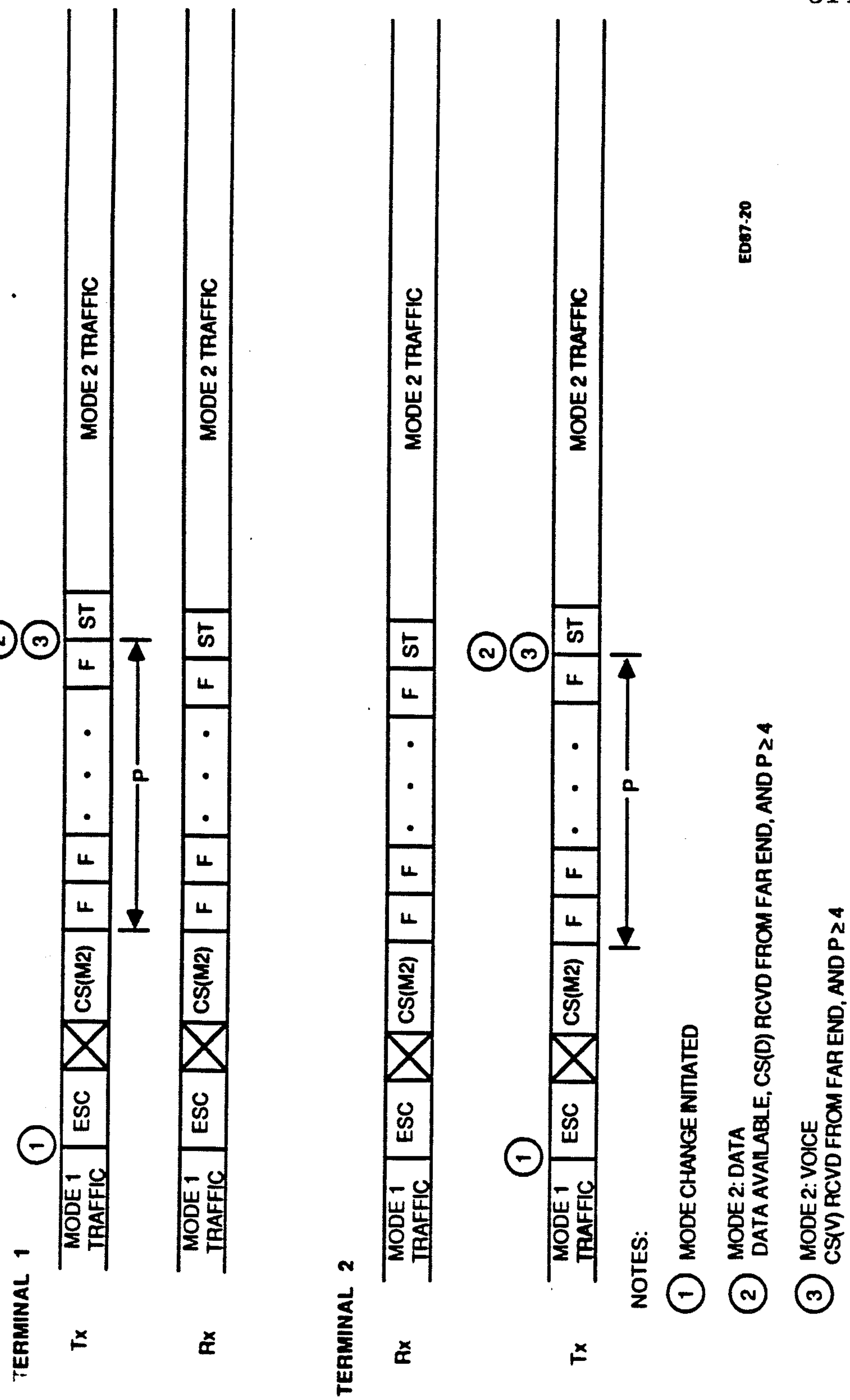


Figure 2-30. Full Duplex Mode Change – Common Mode (Simultaneous) Signaling Diagram

When both carriers have dropped, the initiator in the call setup sequence which failed shall initiate call setup by transmitting the 2100 Hz ESCD tone. Both terminals shall continue by following the standard 2400 bps call setup sequence. In this case, however, the diversion to a V.32 mode by a message A/B exchange shall not be allowed. Accordingly, in response to the 2100 HZ tone the responder shall transmit the standard P1800 signal without phase reversals and call setup at 2400 bps shall continue as shown in Figure 2-3.

This complete restart at 2400 bps is depicted in Figures 2-57 and 2-58.

If a glare condition exists and both terminals transmit the Restart Failed Call message, the restart sequence shall proceed as described above with the original initiator restarting call setup at 2400 bps. If, however, either terminal transmitted the standard failed call message, this transmission shall take precedence over the request to restart and the rules for failed call shall apply.

This restart of call setup shall apply only to the V.32 modes. In the event the call setup in the V.26 2400 bps fails, the terminals shall transmit the standard Failed Call message as defined for the 2400 bps call setup sequence.

2.2.3.1.7 <u>Full Duplex Retrain Request</u> STU-IIIs offering a full duplex V.32 transmission format shall provide the capability to retrain the modem without repeating the entire exchange of call setup messages. The Retrain Request Message (RTR) used as shown in Figure 2-59 shall be used to request retraining. The Retrain Request shall not be transmitted until the terminal has transmitted its own initial CS and received the initial CS from the remote terminal. The retrain request may be made immediately after the CS messages are exchanged or later during traffic.

The retrain request is transmitted by the leader using an ESC/SOM/Retrain Request sequence followed by filler. Upon receiving the Retrain Request the follower transmits ESC/SOM/Retrain NACK followed by filler if it is not willing

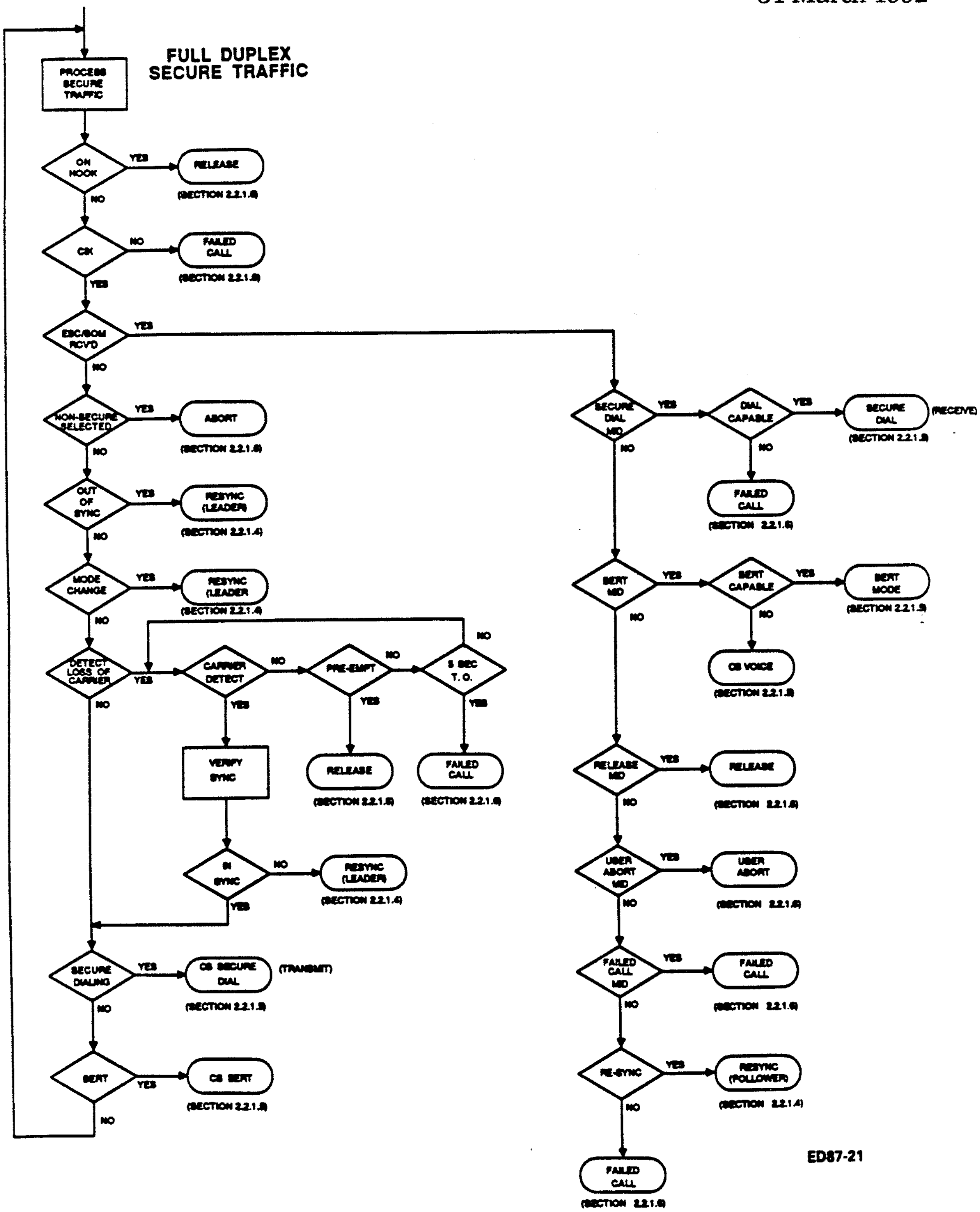


Figure 2-31. Secure Traffic Signaling Sequence Flow Diagram

In addition to the fallback required or allowed after a failure in secure call setup, a terminal may fall back automatically during secure call setup if the terminal estimates that the transmission error rates expected during secure traffic will be too high to achieve useful communication in the selected mode of operation. In the secure voice mode, for example, it is recommended that the terminal fall back to 2400 bps if the expected error rate at 4800 bps is greater than 1 percent. The expected error rates may be predicted during the V.32 modem training sequence, or from the number of errors corrected in the BCH coded messages during secure call setup.

If a terminal that is not eligible for V.32 modem retraining detects a failure before it has completed the transmission of the V.32 Bl segment, it shall cease transmitting. If restart is not indicated, the terminal shall follow its standard sequence for failure at this point in the call setup. If restart is to be performed, the initiator shall wait until both terminals have ceased transmitting and then resume the call setup sequence at 2400 bps by transmitting ESCD. If restart was optional and the responder does not wish to restart, it shall disregard the received ESCD and follow its standard sequence for failure at this point in the call setup.

If a terminal detects a failure after it has transmitted the V.32 Bl sequence it shall transmit Failed Call or Restart Failed Call in accordance with the requirements and options for failing or restarting call setup. Following transmission of Failed Call the terminal shall follow its standard failed call sequence. When Restart Failed Call is selected, the terminal shall assume the role of leader, transmit Restart Failed Call and drop carrier.

If restart is an option the follower may transmit the standard Failed Call message if it receives a Restart Failed Call message and does not wish to Restart. If the follower receives the Restart Failed Call message, and restart is required, or if restart is optional and the follower wishes to restart, then it shall drop carrier and prepare to restart.

The STU-III shall then handle the secure call interruption as necessary. To reduce the probability of a talk-off situation (where an invalid Escape sequence is detected in valid cipher traffic), the terminals should look for ESC followed immediately by SOM before suspending traffic processing. This will require the terminal to provide sufficient buffering to be able to determine if the pattern should be processed as normal traffic, or if it should be treated as an interruption sequence. If the STU-III detects ESC/SOM, and the STU-III does not recognize the following 16 bit as a valid MID, the STU-III shall enter the Failed Call sequence. Where a resync is required, the STU-III returns to the synchronization process described in Section 2.2.1.4. The Failed Call handling is described in Section 2.2.1.6.

2.2.1.5.1 Full Duplex Secure Voice The STU-III shall be capable of transmitting digitized speech securely at 2400 bps. The STU-III voice processor is specified in FSVS-220.

2.2.1.5.2 Full Duplex Secure Data The STU-III shall be capable of transmitting synchronous data securely at 2400 bps. It is intended that any vendor's Type I or Type II STU-III shall be interoperable with any other STU-III in the MER data mode.

2400 bps Synchronous Data. The data mode signaling protocols are initiated whenever the STU-III subscriber activates the Data Mode control, and data is available for transmission as specified in FSVS-220. At this time, the STU-III initiates the Data Mode set-up sequence.

The STU-III shall ensure that the first bit of available data is the first bit encrypted and transmitted after Start is transmitted. There shall be no data bits lost in the encryption/ decryption process (i.e., there will be no sacrifice bits in the data mode caused by the encryption process).

The 2400 bps synchronous data mode does not include:

achieve call setup in the V.32 mode. These capabilities shall be in accordance with the requirements in paragraphs 2.2.3.1.6.1 and 2.2.3.1.6.2 below.

2.2.3.1.6.1 V.32 Modem Training Failures If a terminal detects a failure in the V.32 training sequence before it has completed the transmission of the V.32 Bl segment, it shall enter a V.32 retrain sequence if the mode selected by the Message A/B exchange included the modified V.32 modem training rules. When using the modified V.32 rules, the terminal detecting the failure shall initiate the V.32 modem retrain as specified in Rec. V.32, paragraph 5.5. The V.32 retrain, however, may be performed only once during a single call setup attempt.

A terminal may not be eligible to perform a V.32 retrain, either because one retrain has already been attempted, or because the mode selected in the Message A/B exchange did not include the modified V.32 modem training rules. If such a terminal detects a failure before it has completed transmission of the Bl sequence, it shall be eligible to perform a fallback to the V.26 training sequence in accordance with the requirements specified below.

2.2.3.1.6.2 Call Setup Failure Fallback STU-IIIs offering the full duplex V.32 transmission format shall provide the capability to restart call setup in the V.26 2400 bps mode automatically after a failure to achieve call setup in the V.32 mode.

The automatic restart in the V.26 2400 bps shall be employed after failures due to transmission line quality when the call setup was intended to establish a secure voice call. For secure data, calls with failures due to transmission line quality may be either restarted in the V.26 2400 bps mode or failed at the option of the terminal. The standard failed call sequence shall always be used when the failure is due to incompatible key or other conditions not related to the quality of the transmission media.

- BCH or other error coding or protection while in the data mode
- Out of sync detection and automatic resync initiation by the STU-III while in the data mode.

It is permissible for a STU-III to append up to 127 bits of additional plaintext data (set to all ones) for transmission. The terminal will be capable of accepting an out-of-sync indication externally (i.e. from an external device) that will cause a re-sync sequence. Modem retraining can be initiated manually at any time by the user activating a Non-Secure control (to abort the secure call) and then re-initiating a secure call set-up back into the data mode. This procedure allows the modems to retrain for better error rate performance.

The STU-III will support full or half duplex data devices while operating in the full duplex secure data mode. This will be accomplished using the normal STU-III full duplex transmission format. During the initial synchronization (or a resynchronization) into the data mode, the initiator (leader) and responder (follower) terminals each send the Start message only after data is available for transmission. Thus, it is possible for the secure data traffic to be processed in one direction while there is a continual transfer of Filler (non-secure) in the other direction.

The STU-III, while operating in full duplex mode, shall be capable of supporting independent secure data transfer in both directions. This requires that a STU-III be capable of starting and stopping the secure data transfer in one direction while maintaining a secure data transfer in the other. In this situation, the terminal that initiates the stopping and starting will assume a leader role and transmit an ESC/CS (One-Way Data) message (followed by Filler) in the black transmission stream when there is no longer data available for transmission. This will allow the far-end follower terminal to determine the end of valid data. If the leader terminal determines that there is more data available for transmission, it will again initiate a Start and transfer the secure data, such that the first bit encrypted and transmitted by the STU-III is the first bit of the available data. The signaling for this situation is shown in Figure

The expansion shall also be applied to secure dial digits transmitted at 9600 bps. When secure dial digits are expanded, the expansion shall be performed after all BCH coding and encryption have been completed but before differential encoding.

NOTE: Models of the STU-III with Contractor ID (CID) set equal to "30" will send secure dial digits without dibit expansion.

In the signaling plan defined for 2400 bps operation there is a requirement for the responder or follower to transmit exactly 4 frames of filler between Crypto Sync (CS) and Start (ST) in the secure voice mode when replying to a crypto sync transmitted by the initiator or leader. In other modes the requirement is for a minimum of 4 frames of filler. At 4800 bps this provision is modified to require 9 frames of filler in the secure voice mode between CS and ST and a minimum of 9 frames elsewhere, while at 9600 bps the corresponding requirement is for 19 frames of Filler in the secure voice mode and a minimum of 19 frames elsewhere.

For 2400 bps operation, there is an additional requirement to revert to secure voice operation when mode conflicts arise trying to establish crypto sync. For V.32 operation, this requirement is continued if the terminal contains the voice processor for the transmission rate in effect. If the terminal does not have the required voice processor, then Failed Call shall be used when the mode conflict arises. If a terminal without a voice processor for the established data rate receives a CS voice from the remote end, it shall reply with Failed Call.

2.2.3.1.6 Failures in V.32 Modem Training and Secure Call Setup

STU-IIIs offering the full duplex V.32 transmission format may provide the optional capability to restart V.32 modem training if a failure occures before the terminal has completed modem training. All STU-IIIs offering the full duplex V.32 transmission format, however shall provide the required capability to restart call setup in the V.26 2400 bps mode automatically after a failure to

2-32. Note that both terminals can operate separately, or concurrently in this manner. Also the follower terminal will accept a CS (One-Way Data) message, Filler, and possible subsequent Start message and secure transmission data without performing an end-around resynchronization.

The terminals will use the ESC/CS (Data) to initiate a normal end-around resync as is the case when an out-of-sync indication is provided to the STU-III, or if the STU-III changes modes.

2.2.1.5.3 Full Duplex Secure Dialing The STU-III will be capable of transmitting dialing information securely to a far-end STU-III (or Line Interface Terminal, see Section 2.4) provided the far end is identified as being capable of receiving secure dialing. This capability is indicated by an appropriate status bit in the CAP/SV message. If the far-end terminal indicates that it is not capable of receiving secure dial information but the user attempts to initiate a secure dialing sequence, the STU- III will not enter the secure dialing mode.

After secure traffic is established, the transmitting terminal shall be capable of dialing, as a minimum, any of 16 dial characters (i.e., 0-9, #, *, FO, F, I, P). The transmitting terminal has the option of initiating the secure dialing transmission in two possible ways. The STU-III will adopt at least one (and possibly both) of these approaches.

At the discretion of the vendor's STU-III design, the secure dialing transmission can be initiated as the user depresses a single dial pad key. The signaling design also allows for the terminal to buffer the user's entire dialing sequence. For this dialing method, the STU-III must provide an "end-of-dial" control for the user to initiate the transmission of the dialing information. With either option, the terminal must be capable of transmitting any of the 16 dial characters in any sequence.

At the conclusion of the Bl segment, the V.32 modem shall transfer to the data transmission mode, treating all further messages and traffic defined by FSVS-210 and FSVS-220 as data that is transparent to the V.32 modem.

2.2.3.1.4 Scramblers During the phase of training and mode selection shown in Figure 2-8 within the Note 2 and 3 boundaries, the STU-III shall operate scramblers as specified by the Rec. V.32. Following the completion of the Bl sequences the transmission shall continue with the SOM and CAP/SV sequence shown in Figure 2-11. At the transition between Bl and SOM, the scramblers in the Rec. V.32 shall be discontinued, and scrambling specified for the interoperable 2400 bps mode shall be followed, except that transmission of the messages shall be at the selected transmission rates.

2.2.3.1.5 Signaling Modifications for V.32 Transmission After the transition from the Bl sequence to the SOM, the call setup signaling shall continue exactly as specified for 2400 bps except that the signaling messages shall be transmitted at the rate selected during the rate negotiation process. When transmitting at the 4800 bps rate, the dibit organization of messages defined for V.26 shall be continued with each dibit transmitted in a single baud. For 9600 bps transmission the message dibits shall be padded with a message rate reducing dibit D_R=01.

The addition of the rate reducing dibit shall be done in such a way that the original message dibit sequence D_1 D_2 D_3 ...D_n is modified to D_1 D_R D_2 D_R D_3 D_R...D_n D_R. The expansion shall be performed after all BCH coding and scrambling has been completed but before differential encoding. The expanded dibit sequence shall be grouped into 4 bit nibbles D_1 D_R, D_2 D_R, D_3 D_R... D_n D_R with each nibble transmitted in a single baud at 9600 bps. This expansion shall be performed on: (1) all of the data bearing messages identified in Table 4-1; (2) all of the non-data bearing messages identified in Table 4-1; (3) the supervisory messages SOM, START, EOM, and ESCAPE, and (4) FILLER everywhere except for the FILLER transmitted between Crypto Sync and Start.

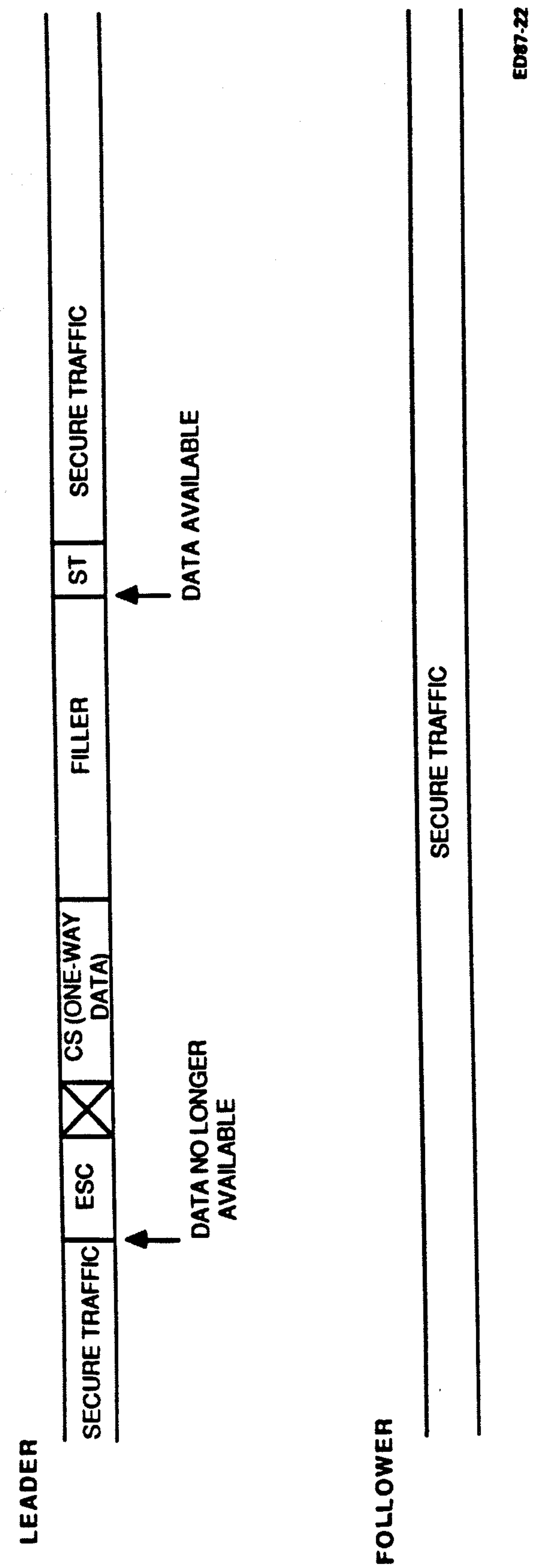


Figure 2-32. Half Duplex Data Device Control Signaling (FDX Mode)

2.2.3.1.2 Message A/B Mode Selection The message A/B exchange shall establish the mode selected by the initiator and responder for the transmission of voice or data traffic. After this exchange both terminals will know the rate selected for traffic and whether the call is for secure data or secure voice.

2.2.3.1.3 V.32 Rate Negotiation During the V.32 start up procedure, the STU-III modems shall engage in the standard V.32 rate negotiation. This will allow the modems to select trellis coding if it is available and desirable, and will allow the rate selected for traffic during the message A/B exchange to be altered by the rate negotiation process. The rate negotiation shall proceed, however, with the assumption that the STU-IIIs will enter the voice or data mode selected by the message A/B exchange. The selection of voice or data shall not be altered during V.32 rate negotiation.

Within the context described above, the answer mode modem shall construct the rate message R1 to include the bits corresponding to the V.32 rates it has available for secure traffic and call setup. The R1 message shall include the rate negotiated during the A/B exchange. If appropriate, the answer mode modem may set bits for an alternate rate or trellis coding.

If the rate message R1 offers only one rate, the remaining rate negotiation messages shall indicate the selected rate.

If the rate message R1 offers alternate rates, the remainder of the rate negotiation shall proceed in accordance with the V.32 protocol taking into account the mode and data rate selected in the Message A/B exchange.

In any of the cases for rate negotiation described in the preceding paragraphs, the selection of trellis coding may be negotiated in accordance with the V.32 protocol.

Secure dialing is only initiated while the terminal is in the secure voice or secure data mode. The transfer of dialing information is sent in one direction; the normal secure voice or secure data traffic in the other direction continues undisturbed, except that LPC voice frames may be replaced by LPC silent frames for the duration of the secure dialing transfer. Figures 2-33 and 2-34 depict the processing and signaling timeline for the full duplex secure dialing sequence, respectively. When a user initiates a secure dialing sequence, the STU-III will transmit Escape (ESC), SOM, a CS (Secure Dial) message, four frames of Filler, and Start. At this point the transmitting STU-III enters secure dialing traffic. The traffic is sent in a BCH-coded format, at an effective 1200 bps information rate. The dialing digits are coded into hexadecimal (4 bit) characters and grouped into 32 characters (to fill a BCH-coded block) for transmission (see Chapter 4 for dialed digit codes). If the STU-III has less than 32 dialing characters, the remainder of the BCH block is filled with null characters. The STU-III may send as many BCH blocks as necessary to transfer the dialing information. It may also send an unspecified number of "null character" frames following the secure dialed digits.

Following the Secure Dialing traffic transmission, the transmitting terminal will transmit Escape (ESC), SOM, a Crypto Sync (One Way) message, Filler (a minimum of four frames) and a Start message to revert to the mode in which the terminal was operating prior to the secure dialing transmission.

Separate CS (One Way, Voice) and CS (One Way, Data) messages are used to indicate to the far-end terminal which mode is selected. It is intended that the terminals restore the mode which was active prior to the dialing transmission. This signaling should not cause an end-around cryptosync; the receiving terminal will detect the ESC/SOM, attain cryptosync, and reenter the appropriate secure mode upon receipt of Start. If there is a mode discrepancy (i.e., the one-way CS received is not the same as the traffic being supported on the follower's transmit line), the terminal acting as the follower for the dialing transmission will be forced to initiate a normal (end-around) resync

Release message and place the line electrically on hook immediately upon detection of the Release message or after some timeout. In the event that there is an incoming transmission when the leader goes on hook, the leader terminal shall wait up to 1.5 seconds before placing the line electrically on hook. During this time, if the incoming carrier is dropped, the leader terminal will transmit the Release message sequence. If carrier is received beyond the 1.5 seconds, the leader terminal will just go electrically on hook without transmitting the Release message.

2.2.2.4.4 ALARM Interruption Sequence If the terminal detects a hardware malfunction, crypto alarm, or security- related software health check failure; the terminal shall either terminate the call by immediately placing the telephone line on hook or enter a Failed Call sequence (depending on the particular terminal's security design). The terminal can be used again for a POTS call, or a secure call if the alarms clear after the user goes on hook or enters the POTS mode.

2.2.3 Alternate Interoperable Modes

Models of the STU-IIIs may offer alternates for interoperable performance in full or half duplex in conformance with the specifications of this section.

2.2.3.1 Full Duplex Operation Using the Rec. V.32 Format

2.2.3.1.1 Modulation Requirements As indicated in paragraph 2.2.1.2, the STU-III may depart to an interoperable V.32 modem. This modem shall conform to the CCITT Rec. V.32 for interoperable use at 4800 and 9600 bps.

Figure 2-8 illustrates the transition into the V.32 modem training sequence. As shown in Figure 2-8, the ESCD/P1800/MSG A/B exchange replaces the 2100 Hz phase of the V.32 standard, while from the start of the AA or AC sequence through to the end of the Bl sequence, the STU-IIIs shall conform to the signaling specified by Rec. V.32.

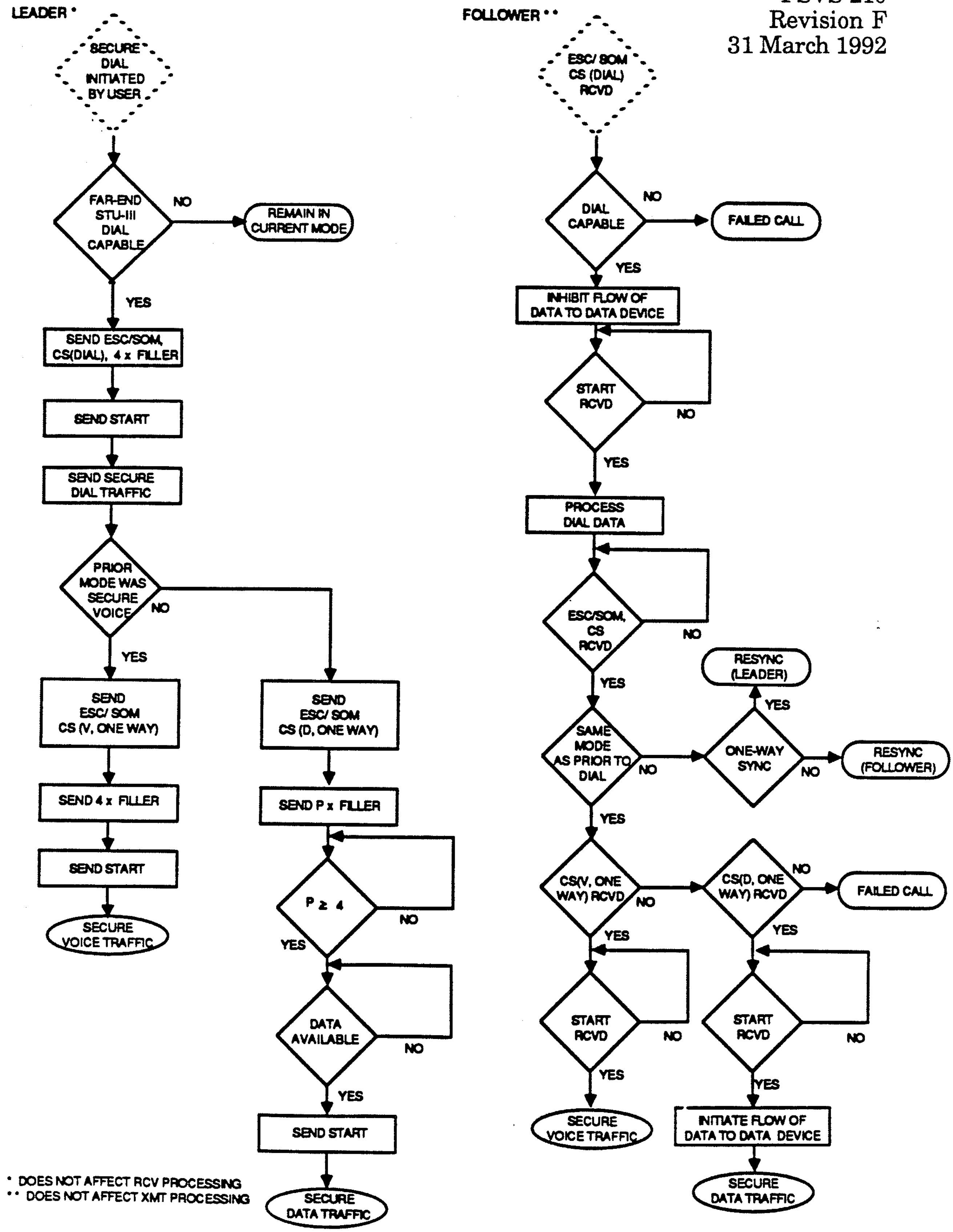


Figure 2-33. Full Duplex Secure Dial Process Flow Diagram

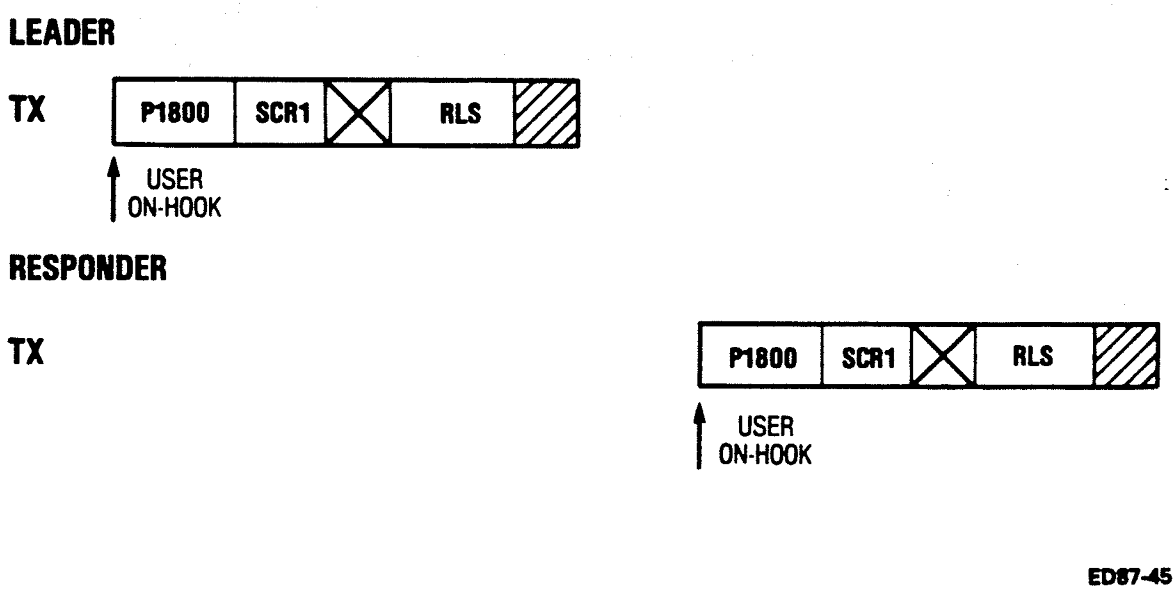


Figure 2-56. Half Duplex Release Signaling Diagram

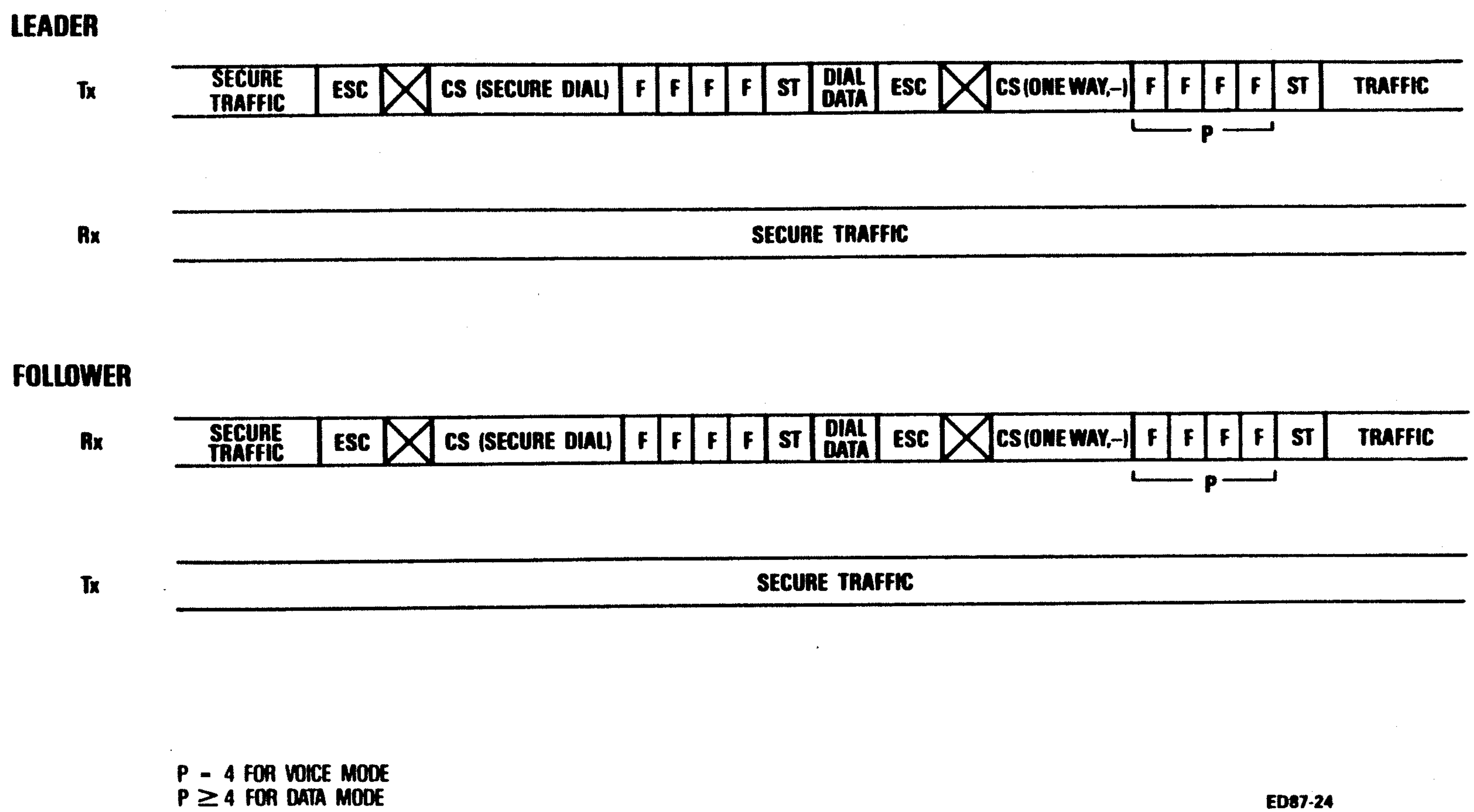


Figure 2-34. Full Duplex Secure Dialing Signaling Diagram

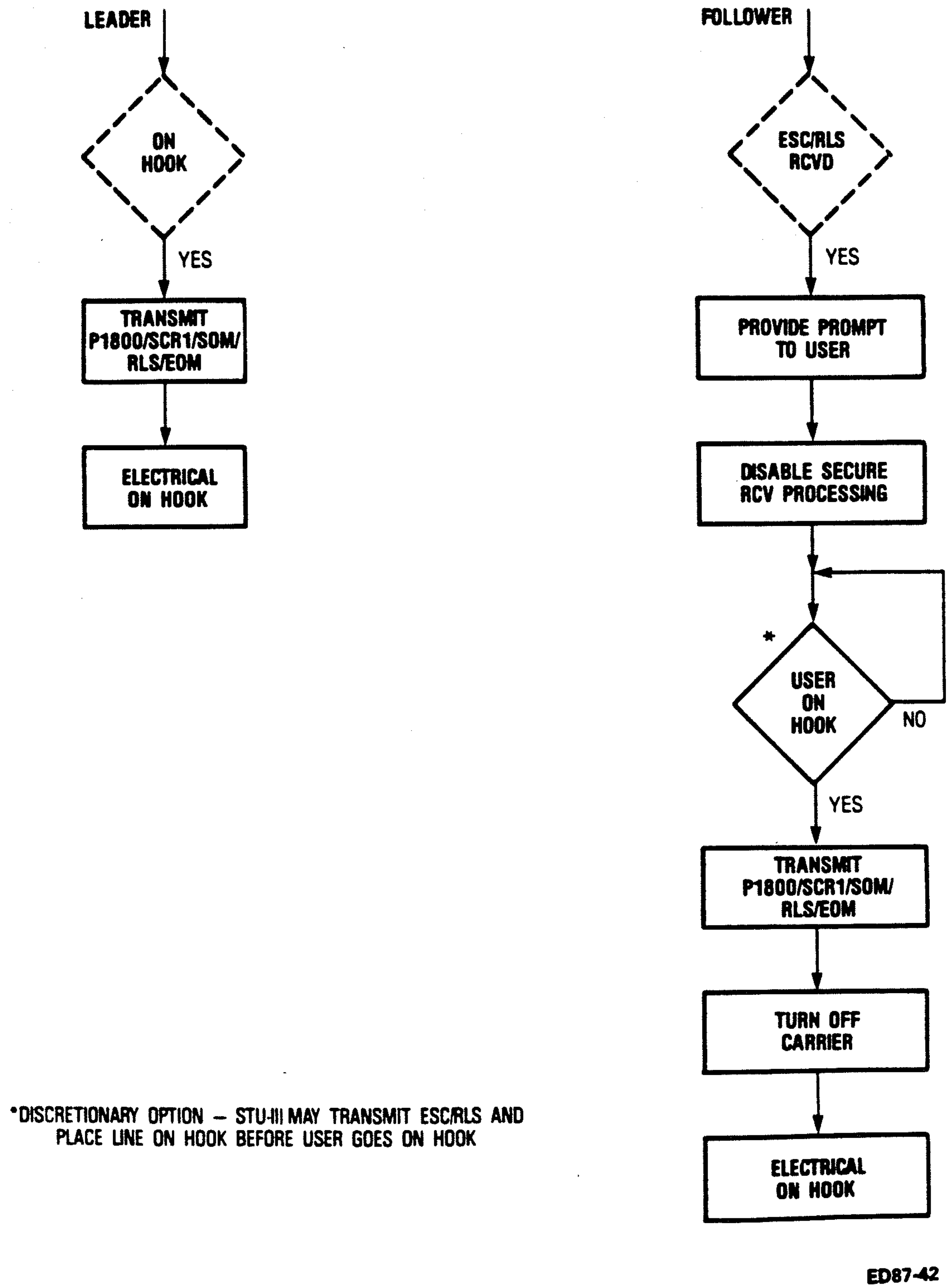


Figure 2-55. Half Duplex Release Processing

procedure. If the follower receives an end-around CS, the follower will proceed with the resync mode change signaling as the follower terminal (Section 2.2.1.4).

2.2.1.5.4 Full Duplex Bit Error Rate Testing (BERT) Provisions The Bit Error Rate Test (BERT) is a discretionary option for the STU-III design. The Signaling Plan does not require a BERT, however, to ensure interoperability, a terminal providing a BERT mode shall provide this mode as specified in the signaling sequence described below. The description focuses only on the signaling aspects necessary to support interoperability. The receive processing needed to implement the mode is beyond the scope of the Signaling Plan.

A terminal with the BERT capability shall set the appropriate status bit in the CAP/SV message. When the BERT-capable terminal is in the secure mode and the user actuates the BERT mode, the terminal will proceed only if the BERT-capability bit was also set in the CAP/SV received from the far-end terminal. If the far end terminal does not support a BERT mode, the near end terminal will disregard the user's action to initiate the BERT.

Figures 2-35 and 2-36 depict the processing flow and signaling timeline, respectively, for the full duplex BERT sequence. When both terminals support the BERT mode, the leader transmits an ESC/SOM, a CS (BERT) message and Filler. As with initial synchronization, signaling for the BERT mode is compelled such that the leader will continue to transmit Filler until it receives the CS (BERT) from the far-end or times out. The leader may retransmit the CS (BERT) message. A maximum number of attempts for retransmission of the CS message after a timeout (including no attempts) may be established at the vendor's option. If this maximum is reached, the terminal shall go to Failed Call. When the leader receives the CS (BERT) message, the leader transmits Start, followed by encrypted zeros. The follower, upon receipt of CS (BERT) from the leader, transmits CS (BERT) followed by a minimum of four frames of Filler, Start and then encrypted zeros. The terminals shall transmit encrypted zeros until either user terminates the mode or otherwise interrupts the call.

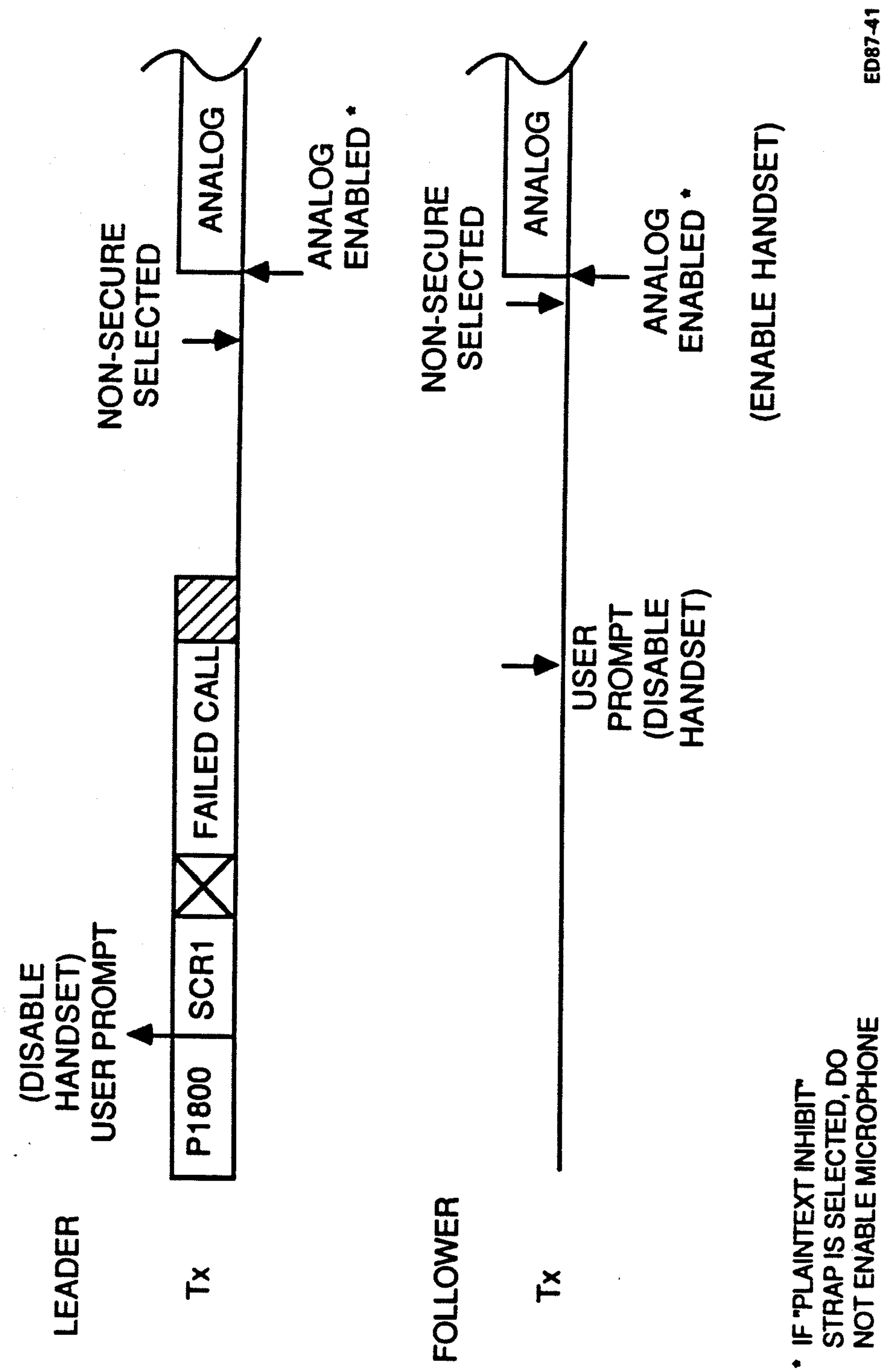


Figure 2-54. Half Duplex Failed Call Processing Signaling Diagram

2.2.1.5.5 Asynchronous Full Duplex Data It is recommended that the STU-III be capable of supporting full duplex asynchronous data modes. If the STU-III incorporates an interoperable asynchronous data mode, it should be one of the following modes: 1200 bps asynchonous half-rate, 1200 bps asynchronous full-rate, or 2400 bps asynchronous full-rate. The asynchronous data mode shall support a 10 bit character format including 1 start bit, 8 data bits, and 1 stop bit. The interface shall support a nominal 1200 bps or 2400 bps data rate. The STU-III shall have a format conversion mechanism consistent with CCITT V.26 to convert asynchronous data to a synchronous bit stream for transmission. The synchronous bit stream is then transmitted to the far-end terminal in 2400 bps full duplex, half-rate BCH-coded format or non-encoded format depending on the mode selected.

There shall be no data bits lost in the encryption/ decryption process (i.e., the first bit out of the data device shall be the first bit encrypted, and shall be the first bit transmitted; there shall be no sacrifice bits in the data mode caused by the encryption process). The STU-III interface to a data device shall be the same for the async data modes as for the synchronous data mode as defined in FSVS-220. Neither the encryption or decryption process shall introduce inversions in the plaintext data stream. It is permissible for the STU-III to append up to 127 bits of additional plaintext data (set to all ones) for transmission.

2.2.1.6 Full Duplex Call Interruption Processing

There are a number of situations that may occur to interrupt the normal processing of a call. These include:

- User initiating abort of the call processing (User Abort)
- Transmission signaling failure (Failed Call)
- User going on hook (Release)
- Hardware malfunction or equipment alarm (Alarm)

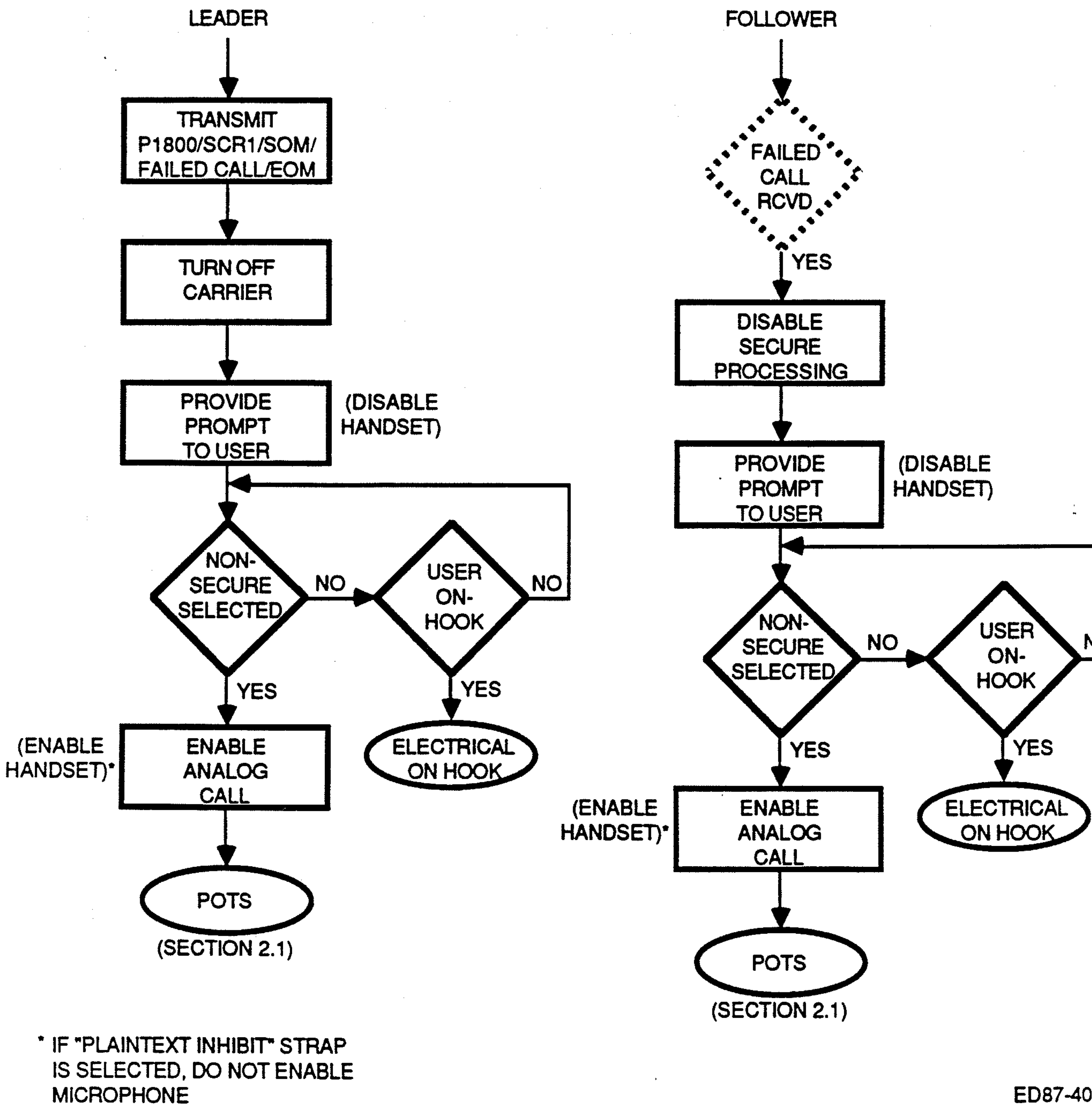
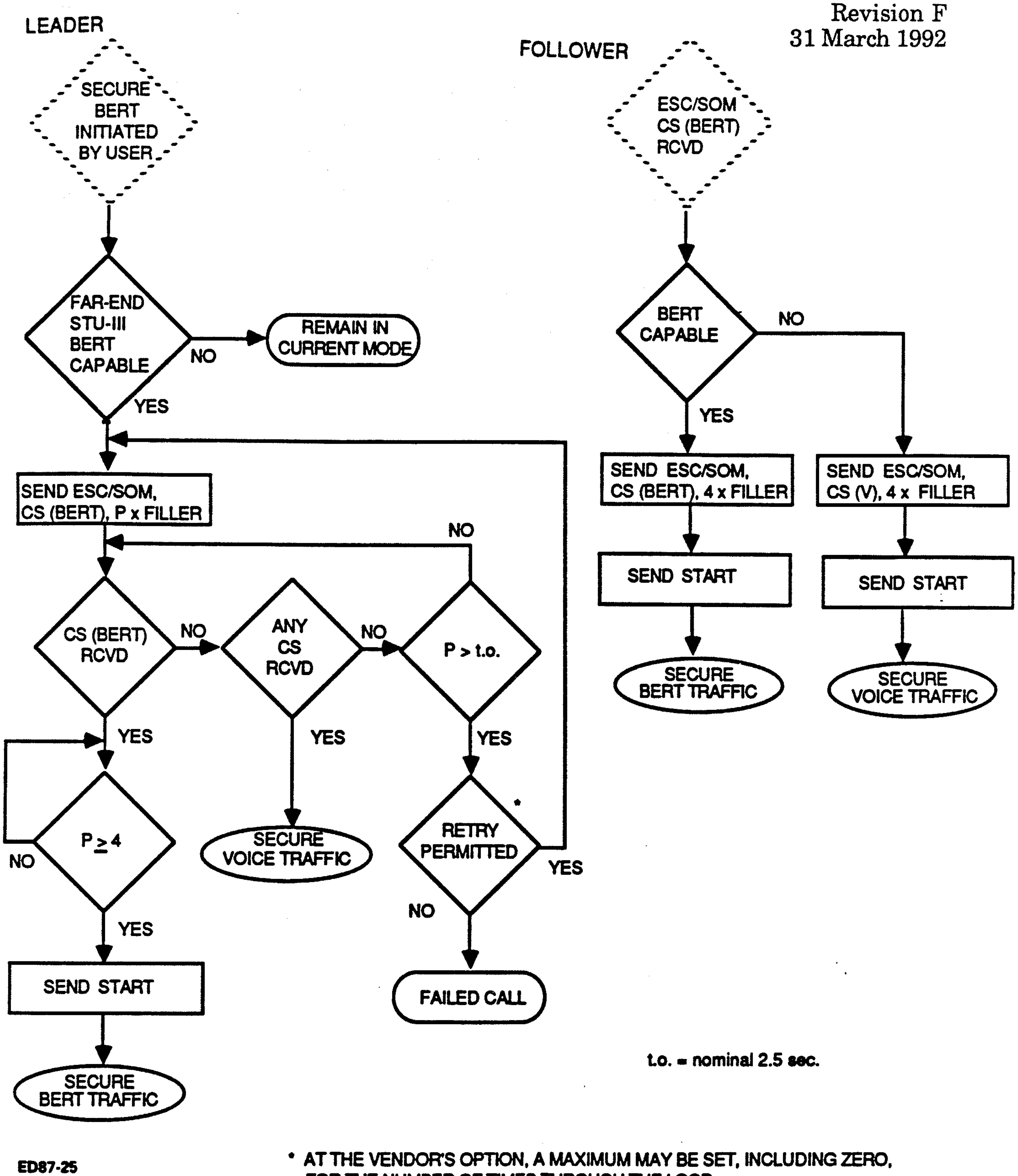


Figure 2-53. Half Duplex Failed Call Processing



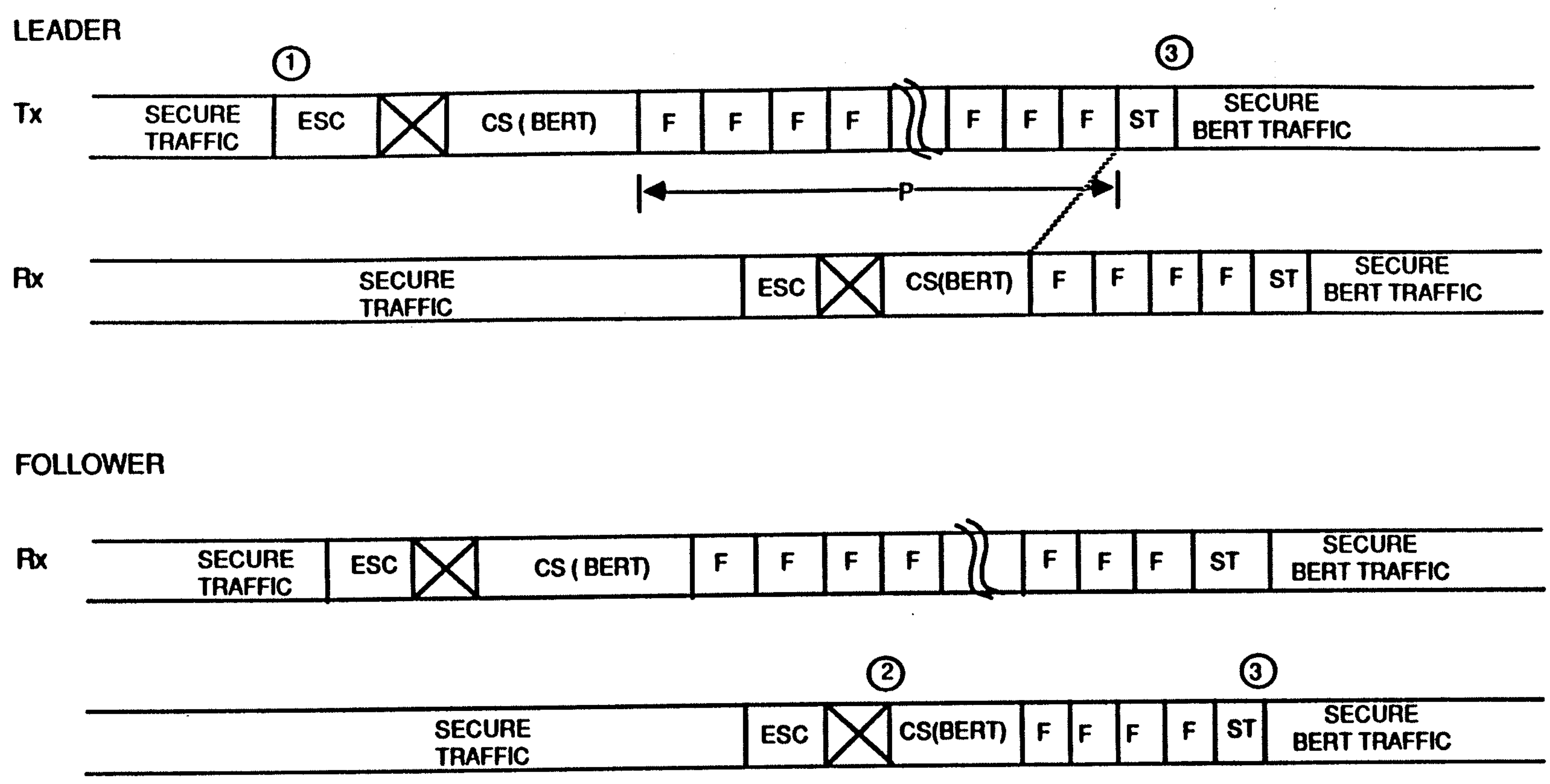
* AT THE VENDOR'S OPTION, A MAXIMUM MAY BE SET, INCLUDING ZERO, FOR THE NUMBER OF TIMES THROUGH THE LOOP.

Figure 2-35. Full Duplex Secure BERT Process Flow Diagram

2.2.2.4.2 Half Duplex Failed Call Interruption Sequence Unless an alternative response is defined elsewhere in the Signaling Plan, the STU-III shall follow the Failed Call sequence if it encounters an uncorrectable transmission or parity error, timeout, or other condition that prohibits normal operation. The terminal detecting the failure assumes the leader role,transmits P1800, 3202, SCR1, SOM, the Failed Call message and EOM, drops carrier, and provides a prompt to the user as defined in FSVS-220. The user can activate his non-secure control and revert to a clear call or go on hook to terminate the call. Figures 2-53 and 2-54 depict the flow sequence and timeline for the Failed Call signaling.

The follower terminal, upon detection of the Failed Call message, also drops carrier and provides a prompt to the user as defined in FSVS-220. Again this user may activate his non-secure control and initiate an analog clear call. Each terminal will only connect its handset to the line after the user has manually activiated his non-secure control. Once a clear call is reestablished, either user can reinitiate a secure call set-up. Again, if the half duplex mode is selected, the STU-III shall provide the capability for the user of the leader terminal to retransmit an Abort message sequence as discussed above (e.g., by reactivation of the non-secure control).

2.2.2.4.3 Half Duplex Release Interruption Sequence The STU-III will follow the release sequence at the completion of a call. If the user is the first to place the handset on hook, the STU-III will transmit P1800, 3202, SCR1, SOM, RLS and EOM, and then place the telephone line electrically on hook. Figures 2-55 and 2-56 depict the flow sequence and timeline for the Release signaling. If the terminal detects the Release message, it will disable the secure processing, provide a prompt to the user as defined in FSVS-220 and, when the user places his handset on hook, will transmit a Release message and place his telephone line electrically on hook. As a design option, the STU-III may transmit a



1. LEADER INITIATES SECURE BERT MODE
2. FOLLOWER DETERMINES SECURE BERT MODE FROM CS (BERT)
3. FIRST BIT OF TRAFFIC MARKED BY HAVING :
   A) SENT CS(BERT) AND WAITED AT LEAST 4 FRAMES OF FILLER
AND B) RECEIVED CS(BERT)

Figure 2-36. Full Duplex Secure BERT Signaling Diagram

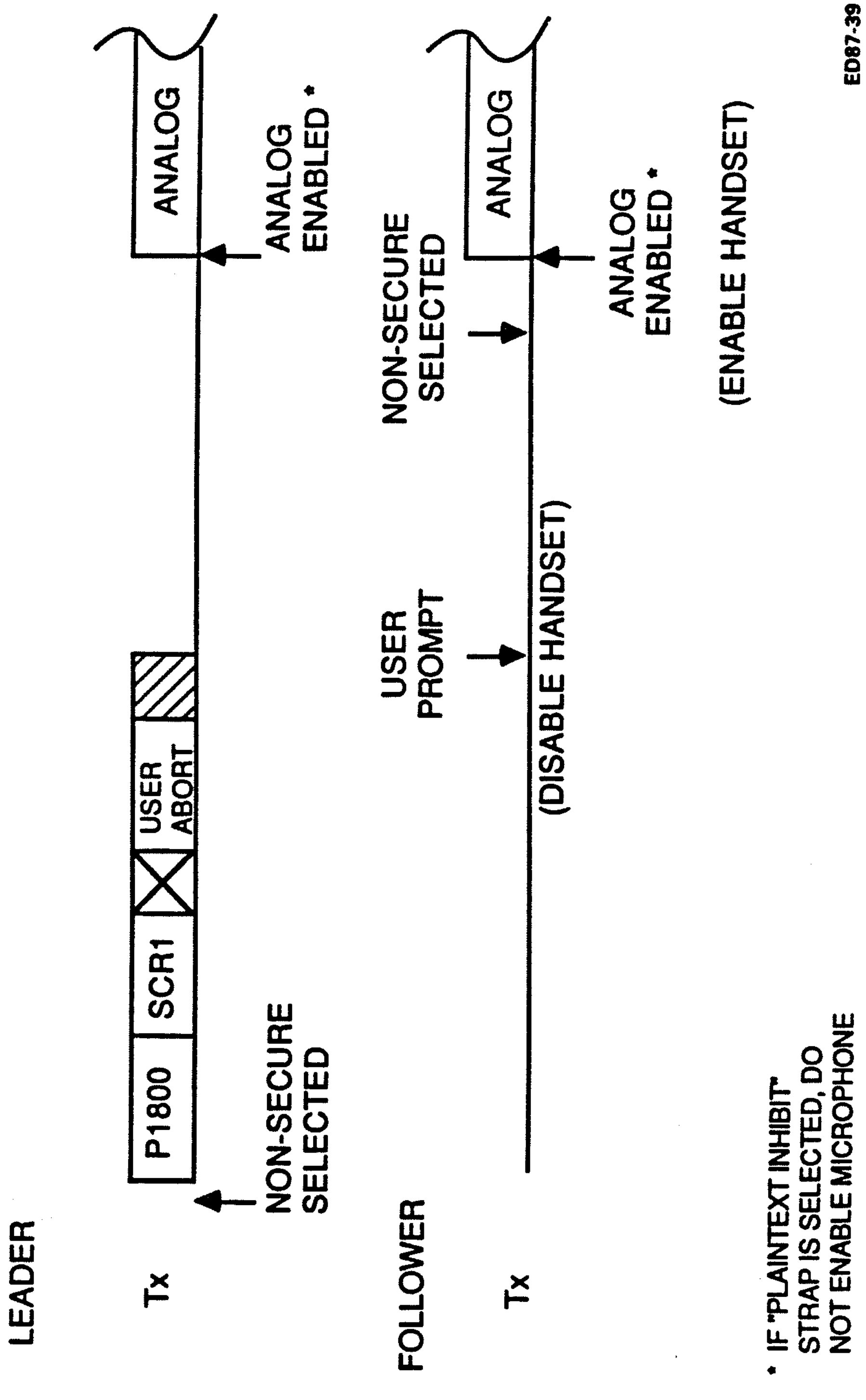


Figure 2-52. Half Duplex User Abort Processing Signaling Diagram

This section describes the full duplex signaling required by the STU-III during each of these situations.

The primary signaling strategy is for the "leader" terminal (initiating the interruption) to transmit a pre-defined unencrypted Escape pattern followed by a message indicating the particular situation (e.g., ESC/Release, ESC/Abort). The far-end, "follower" terminal will detect the message sequence, interrupt the secure call or set-up, and process the interruption appropriately. The message signaling is only used if the interruption occurs during the secure call set-up or while processing secure traffic. For this purpose, the beginning of call set-up for the full duplex mode is defined as the transmission of the first SOM dibit of the CAP/SV message. From this point through the secure call, each terminal shall perform a continuous (dibit synchronous) search of the Escape pattern within the received (black) transmission bit stream. The Escape signal must be detected in background or cipher with a talk-off specification of 1000 hours (mean recurrence interval). If the talk-off occurs during the secure call set-up, the STU-III shall enter the Failed Call state; otherwise the STU-III shall re-sync into the same mode. It is recommended that the STU-III should not perform any action if a talk-off occurs during a resync signaling sequence. The STU-III may, as an option, detect the SOM after the Escape pattern to reduce the probability of a talk-off condition. The signaling for ESC/SOM detection is defined in Section 2.2.1.5. If a call interruption sequence occurs before the CAP/SV SOM, the STU-III will turn off the modem carrier (if the terminal is currently transmitting a modem signal) and bypass any Escape message transmission. Both STU-III users shall be required to activate the non-secure control and enter the analog call state. Aside from the inhibiting of any message transmission, the terminal operation will be described as below.

2.2.1.6.1 Full Duplex User Abort Interruption Sequence The STU-III will enter a User Abort sequence when the user at either end activates his non-secure control. The intent is to permit the users to revert to a clear (nonsecure) analog telephone call. The clear call is only permitted after each of the users physically initiates the request (e.g., by activating an appropriate non-secure

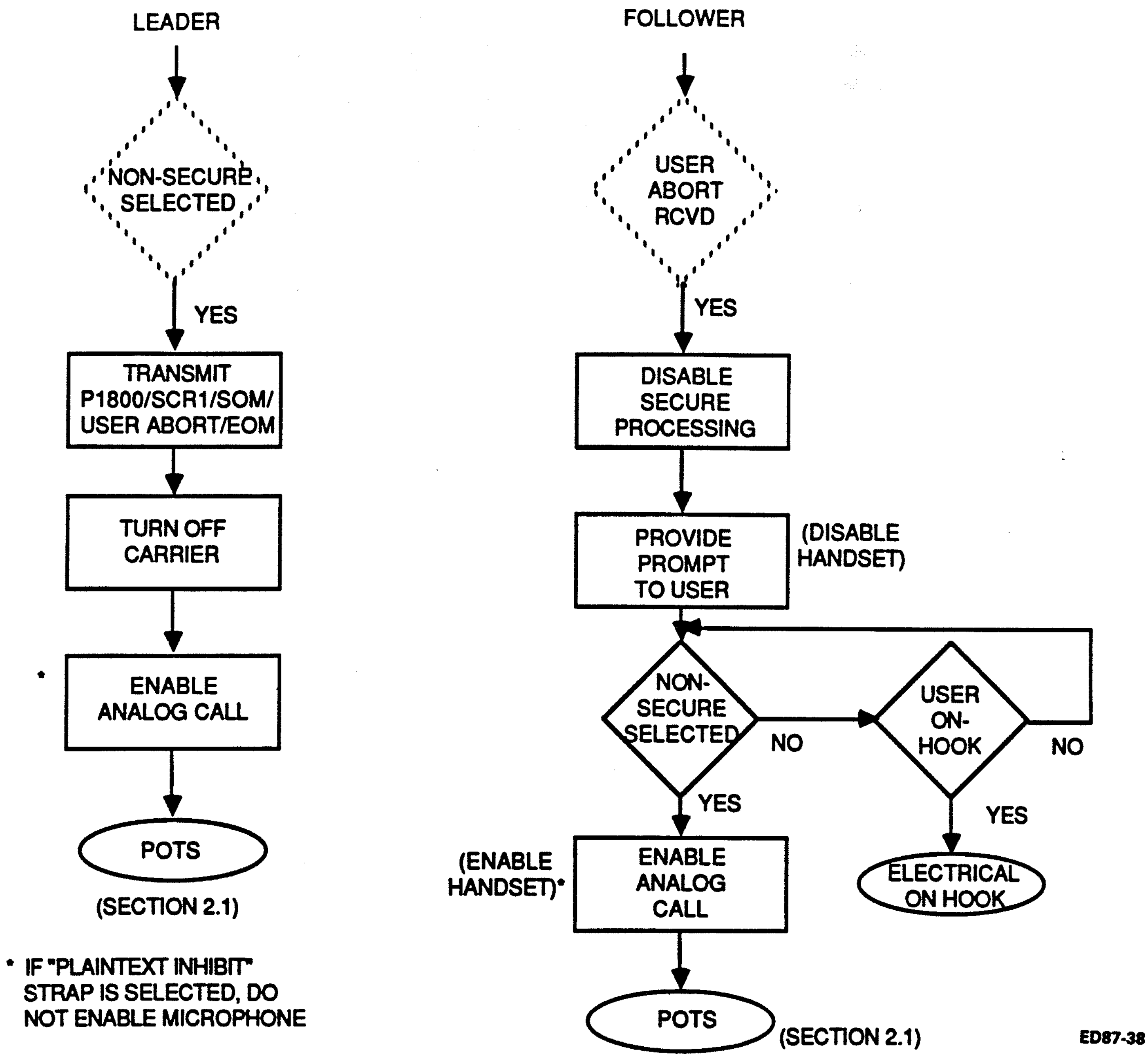


Figure 2-51. Half Duplex User Abort Processing

control). As described during the secure processing earlier, when the user activates the non-secure control, the STU-III will assume a leader role and transmit an Escape/User Abort message, then revert to a clear call. The other terminal assumes the follower User Abort role. The follower terminal will turn off its carrier, alert the user to the User Abort sequence and wait for the user to activate his nonsecure control reverting the call to a clear telephone call. The processing flow and timeline are depicted in Figures 2-37 and 2-38, respectively. Once a clear call is established, the user at either STU-III can initiate another secure call set-up.

2.2.1.6.2 Full Duplex Failed Call Interruption Sequence Unless an alternative response is defined elsewhere in the Signaling Plan, the STU-III shall follow the Failed Call sequence if it encounters an uncorrectable transmission or parity error, timeout, loss of received carrier for more than five seconds, or other condition that prohibits normal operation. The terminal detecting the failure assumes the leader role, transmits an ESC/Failed Call message, drops carrier, and provides a prompt to the user. The user can activate his non-secure control and revert to a clear call. The follower terminal, upon detection of the ESC/Failed Call message also drops carrier and provides a prompt. Again, this user may activate his non-secure control and complete the clear call. Each terminal will only connect its subscriber handset to the line after the user has manually activated his non-secure control. Once a clear call is reestablished, either user can reinitiate a secure call set-up. Figure 2-39 and 2-40 depict the processing flow and timeline for the Failed Call signaling, respectively.

2.2.1.6.3 Full Duplex Release Interrupt Sequence The STU-III will follow the release sequence at the completion of a call. If the user is the first to place the handset on hook, the STU-III will transmit an ESC/Release (ESC/ RLS) and then place the telephone line electrically on hook. If the terminal detects the ESC/RLS, it will disable the secure processing, provide a prompt to the user and, when the user places his handset on hook, will transmit an ESC/RLS and place his telephone line electrically on hook. Figure 2-41 and 2-42 depict the telephone call. The analog clear call at each terminal is only permitted after the user at that terminal physically activates the control (e.g., by activating an appropriate non-secure control).

When the user activates the non-secure control, the terminal will assume the leader role and transmit P1800, 3202, SCR1, SOM, the User Abort message, and EOM as depicted in the flow diagram and timeline of Figures 2-51 and 2-52, respectively. Chapter 4 fully defines the message structure and content. The other terminal assumes the User Abort follower role. The follower terminal will turn off its carrier, alert the user as defined in FSVS-220, and wait for the user to activate his non-secure control. The user may activate his non-secure control to revert the call to a clear telephone call or go on hook. Once the clear call is re-established either terminal can initiate another secure call set-up.

The intent of Half Duplex User Abort signaling is to ensure that the follower does receive the User Abort message. Two design approaches are acceptable:

- In order to ensure that an analog clear call is established or reestablished following an interruption, (i.e., User Abort or Failed Call) in the half duplex mode, the leader terminal may retransmit the User Abort message sequence each time the user activates his non-secure control. This provides the leader with the capability for continually prompting the follower to revert to the clear call in the event that the follower did not receive the User Abort message.

- A terminal shall only be required to transmit the User Abort sequence once if it provides the capability to 'save' the command from the user to go non-secure and delay transmission of the User Abort message until the leader terminal determines that telephone line is clear of all modem signals from the distant (follower) end.

processing flow and timeline for the Release signaling, respectively. At the discretion of the specific terminal design, the STU-III may transmit ESC/RLS and place the line electrically on hook immediately upon detection of ESC/RLS or after some timeout.

2.2.1.6.4 ALARM Condition If the terminal detects a hardware malfunction, crypto alarm, or security-related software health check failure; the terminal shall either terminate the call by immediately placing the telephone line on hook or enter a Failed Call sequence (depending on the particular terminal's security design). The terminal can be used again for a POTS call, or a secure call if the alarms clear after the user goes on hook or returns to POTS mode.

2.2.2 Half Duplex (2400 bps) Operation

The half duplex mode has been included in the STU-III terminal to serve as a back-up option when telephone lines are encountered which cannot support full duplex operation (e.g., excessive echo, or echo-suppressors that cannot be disabled). As with the full duplex mode, the user goes off hook and dials the far end subscriber. The half duplex mode must be selected manually by either the calling or called party. It may be selected prior to dialing or during the analog call (initially or following User Abort or Failed Call sequence) but must be selected prior to either user initiating a secure call set-up. If the appropriate straps are set, the STU-III will support Auto-Secure and/or Plaintext Inhibit for half duplex operation in a fashion similar to that for full duplex. The terminal will exchange variables, attain synchronization and support secure voice, data, dialing or BERT testing operation, using the half duplex protocols specified in this section. During all half duplex transmission sequences, the STU-III will have to monitor the telephone line to verify that incoming carrier is not present before any transmission is initiated. After any half duplex transmission, the terminal must drop modem carrier within 50 ms after the transmission of an unencrypted EOM. After carrier is dropped, both terminals must wait a minimum of 35 ms prior to transmitting in order to allow the far

2.2.2.4 Half Duplex Call Interruption Processing

In the half duplex mode, as in the full duplex mode, there are a number of situations which may occur during the call setup or secure modes of operation which can interrupt the call. These include:

- User initiating abort of the call processing (User Abort)
- Transmission Signaling failure (Failed Call)
- User going on hook (Release)
- Hardware malfunction or equipment alarm (Alarm)

This section describes the half duplex signaling required by the STU-III during each of these situations.

The primary signaling strategy in the half duplex mode for all call interruptions is to send P1800, the 3202 transition dibit sequence, SCR1 (32 dibits), SOM and an appropriate non-data bearing message indicating either a User Abort, Failed Call or Release situation. These transmissions will be initiated during the call setup or the secure mode of operation for any interruption occurring after the beginning of the secure call setup. If the terminal is in the process of transmitting either call set-up messages or secure traffic, it will interrupt the transmission by transmitting EOM, dropping carrier within 50 ms for a minimum of 35 ms, then sending P1800, 3202, SCR1,SOM, the appropriate non-data bearing message, and EOM followed again by dropping of the modem carrier. The beginning of call set-up for the half duplex mode is defined as the initiator activating a secure control. The processing necessary to support call processing interruptions is discussed below.

2.2.2.4.1 Half Duplex User Abort Interruption Sequence The STU-III will enter a User Abort sequence when the user at either end activates a non-secure control. The intent is to permit the users to revert to a clear (non-secure)

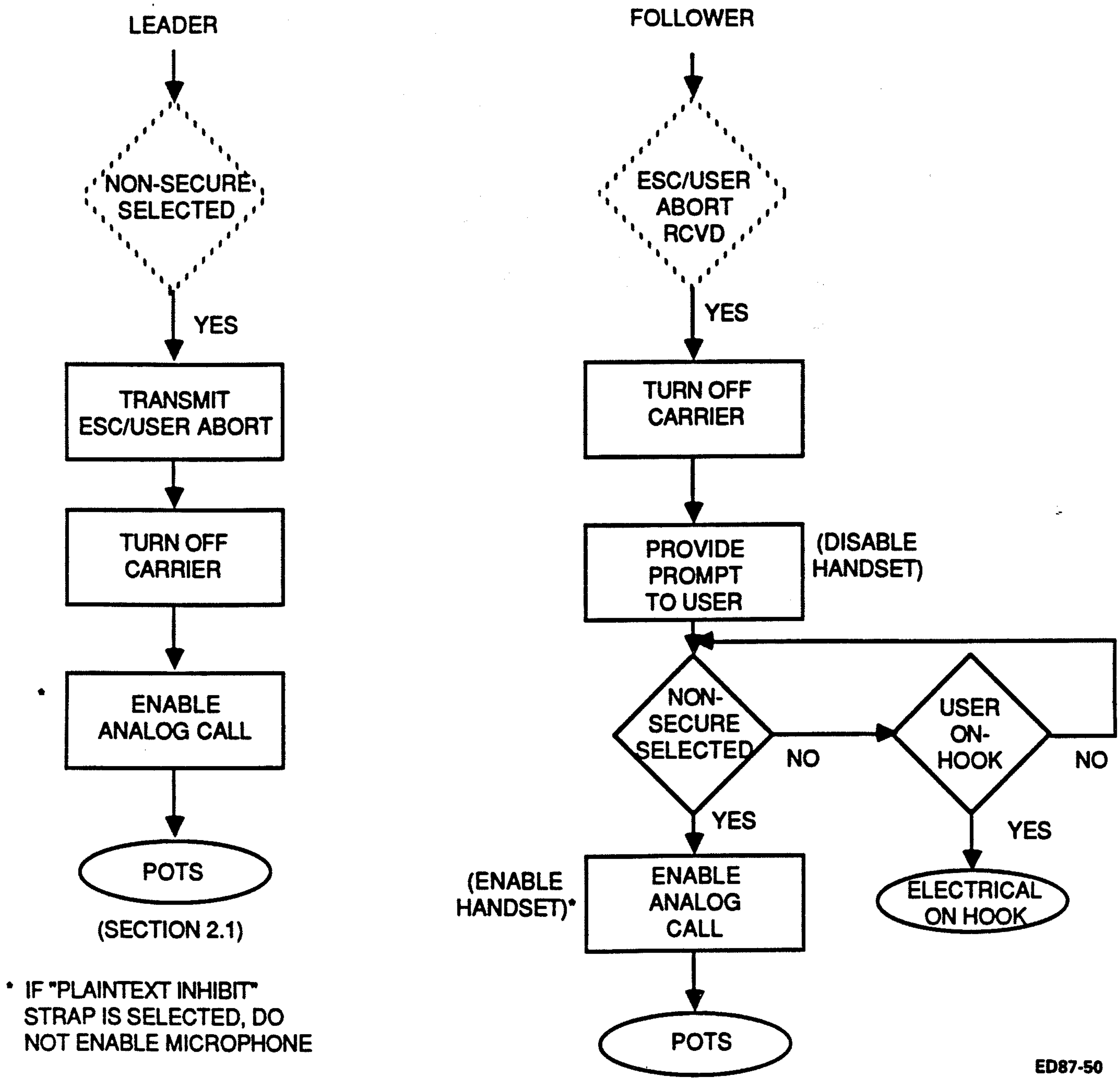


Figure 2-37. Full Duplex User Abort Processing

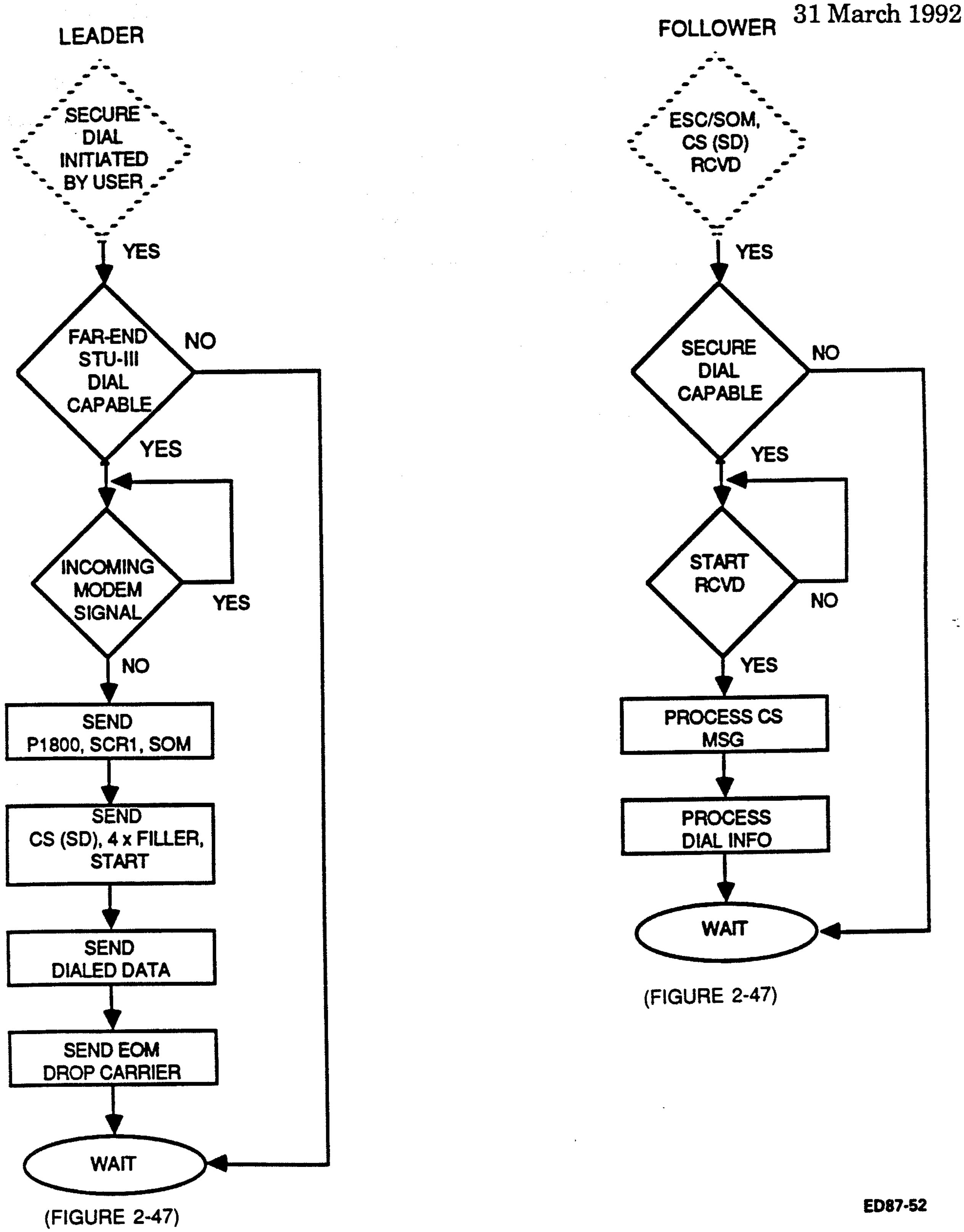


Figure 2-50. Half Duplex Secure Dialing Sequence Flow Diagram

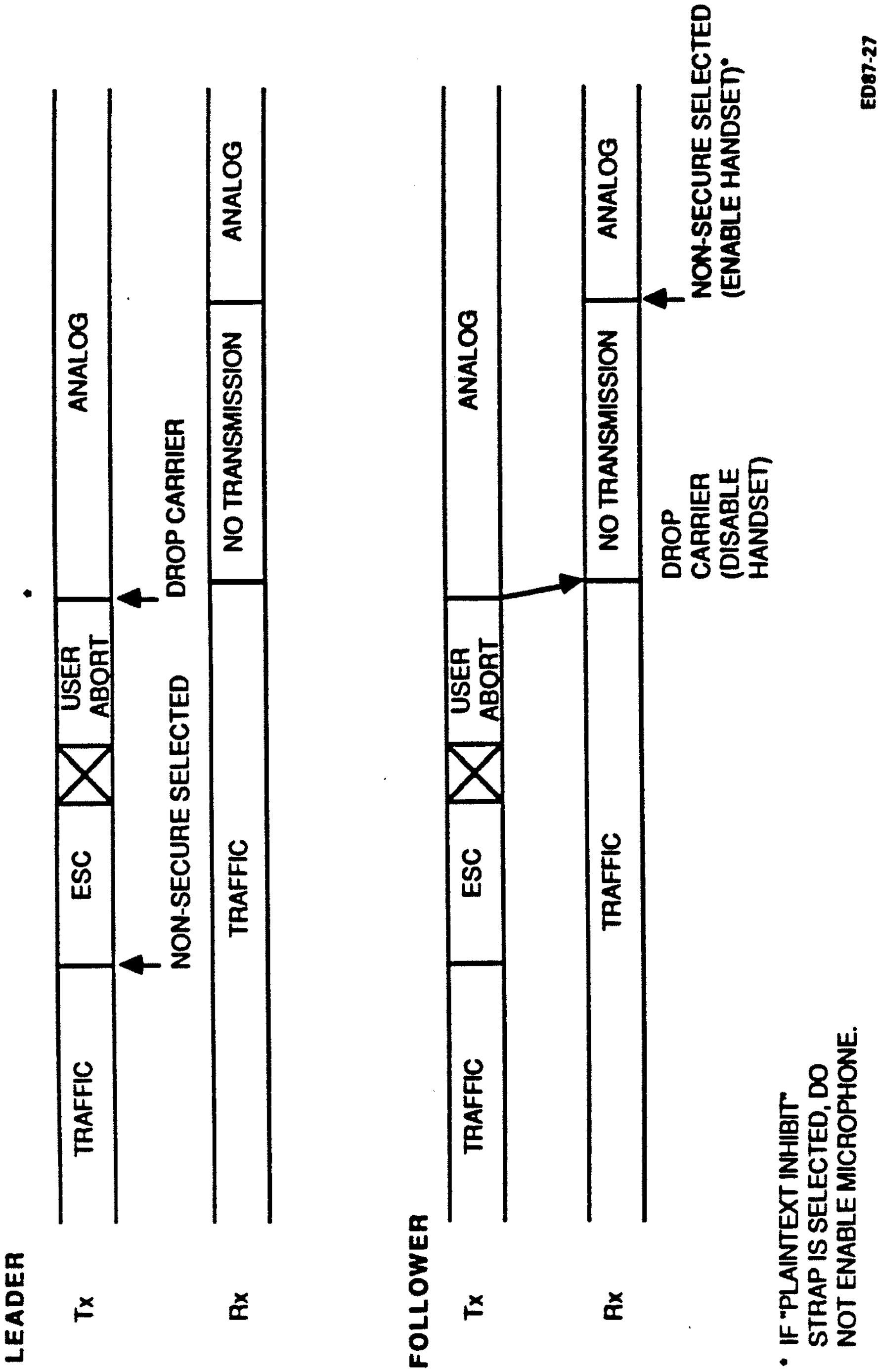


Figure 2-38. Full Duplex User Abort Sequence Signaling Diagram

When a user initiates a secure dialing sequence, the STU-III shall initiate a half duplex Secure Dial transmission, as depicted in the process flow diagram presented in Figure 2-50. The STU-III shall transmit P1800, 3202, SCRl, SOM, a CS (Secure Dial) message, four frames of Filler, and Start. At this point the leader STU-III shall enter secure dialing traffic. The STU-III shall send the traffic in a BCH-coded format, at an effective 1200 bps information rate. The dialing digits shall be coded into hexadecimal (4 bit) characters and grouped into 32 characters (to fill a BCH-coded block) for transmission (see Chapter 4 for dialed digit codes). If the STU-III has fewer than 32 dialing characters, the STU-III shall fill the remainder of the BCH block with null characters. The STU-III may send as many BCH blocks as necessary to transfer the dialing information. It may also send an unspecified number of "null character" frames following the secure dialed digits. The STU-III shall complete the transmission with an unencrypted EOM, and then drop carrier within 50 ms.

Once the Secure Dial transmission is completed, the STU-III shall revert to its normal half duplex operation.

2.2.2.3.4 <u>Half Duplex Bit Error Rate Test (BERT) Provisions</u> The BERT mode for half duplex applications, as for the full duplex BERT mode, is discretionary. When the BERT mode is provided, it shall be designed as described below for half duplex operation. The description focuses only on the signaling aspects necessary to support interoperability. The receive processing needed to implement the mode is beyond the scope of the Signaling Plan.

A terminal with BERT capability shall set the designated BERT bit in the CAP/SV message to a "1". When both terminals support a BERT mode, the signaling shall proceed with the leader terminal transmitting the half duplex preamble, SOM, CS (BERT), four frames of Filler and Start followed by encrypted zeros for a nominal duration of 10 seconds (minimum must be ten seconds) and an unencrypted EOM. Upon receipt of this message the follower terminal shall transmit the same message sequence. Either terminal user may then reinitiate the BERT, or any other mode.

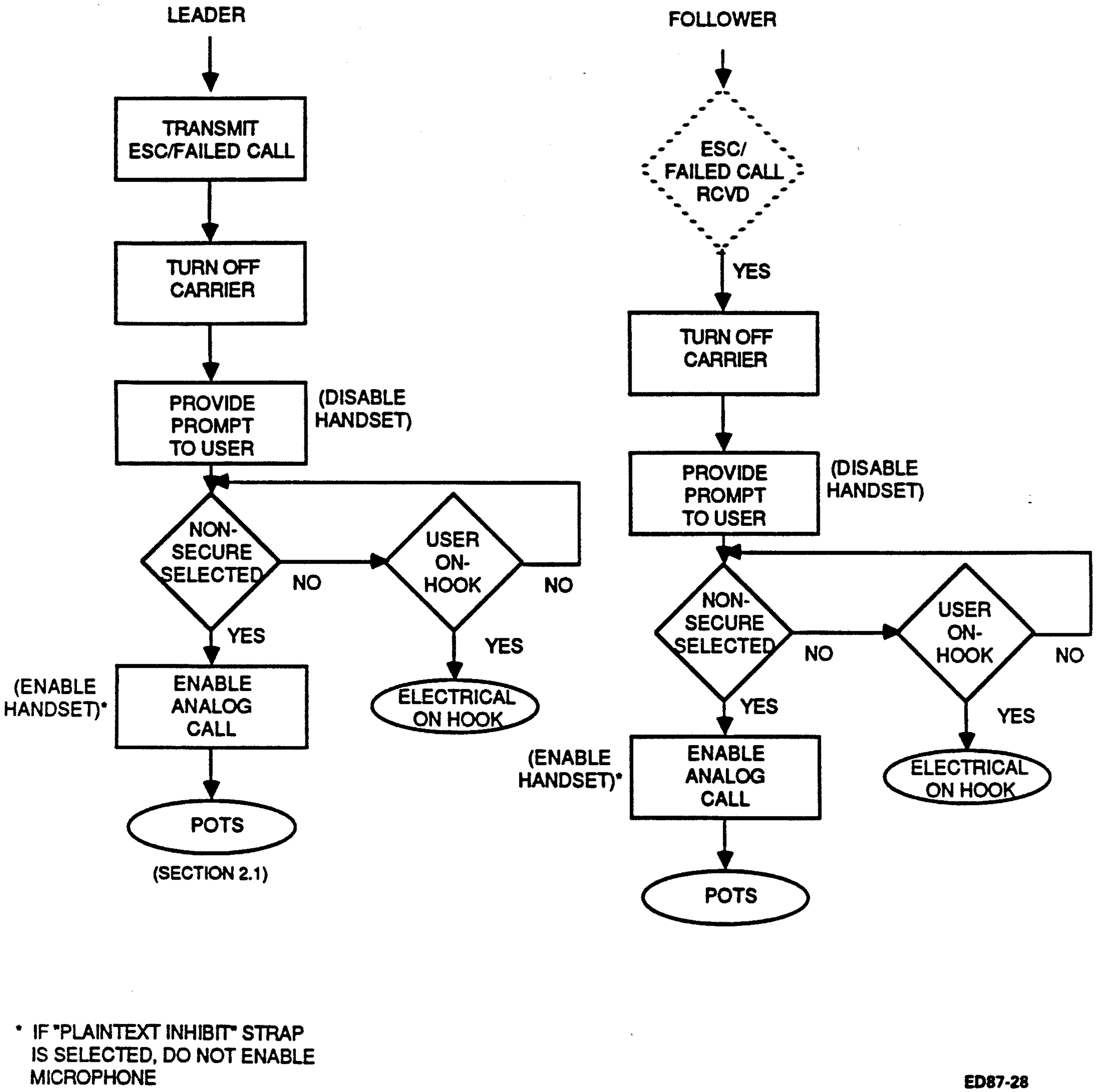


Figure 2-39. Full Duplex Failed Call Processing

Note that all data must be transmitted prior to the EOM transmission. It is also permissible for a STU-III to append up to 127 bits of additional data (set to all ones) before sending EOM. Note that in the half duplex mode a terminal may transmit data even though the far-end terminal is not ready to receive the data. In this case, the user receiving the data has the option of terminating the call or waiting until the data transmission is complete. The receiving STU-III is not required to process the data in this case. The receiving STU-III shall be capable of identifying the end of the received data traffic by detecting the EOM and loss of modem carrier. There are no constraints on the format or content of the data. It is possible that an EOM could occur fortuitously in the transmission bit stream; therefore, there could be a talk-off problem if loss of carrier is not also a criterion in determining the end of the data transmission.

2.2.2.3.3 Half Duplex Secure Dialing The STU-III shall be capable of transmitting dialing information securely to a terminal identified as able to receive secure dialing (as indicated in the CAP/SV message). If the far-end terminal indicates that it is not capable of receiving secure dial information but the user attempts to initiate a secure dialing sequence, the STU-III shall not enter the secure dialing mode.

The half duplex secure dialing can be initiated after the terminals have completed the variable exchange. There are two possible sequences that the STU-III may use to initiate the transfer of the dialed digits as discussed below. The STU-III shall adopt at least one of these approaches.

At the discretion of the STU-III vendor, the secure dialing transmission may be initiated as the user depresses a single dial pad key. Alternatively, the design may allow the STU-III to buffer the user's entire dialing sequence prior to transmission. For this dialing method, the STU-III must provide an "end of dial" control for the user to initiate the transmission of the dialing information. With either design, the terminal shall be capable of transmitting any of the 16 dial digits in any sequence.

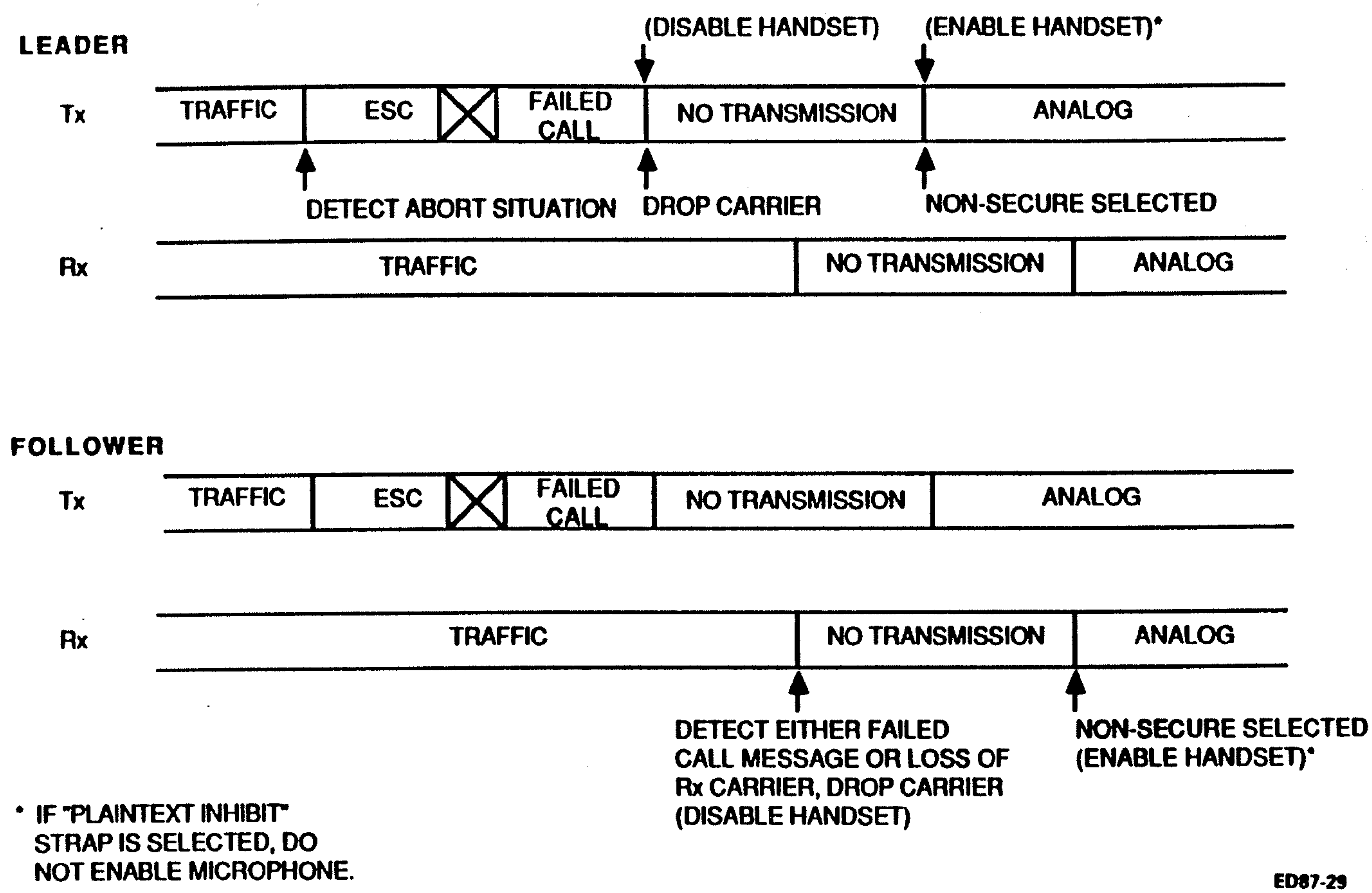


Figure 2-40. Full Duplex Failed Call Signaling Diagram

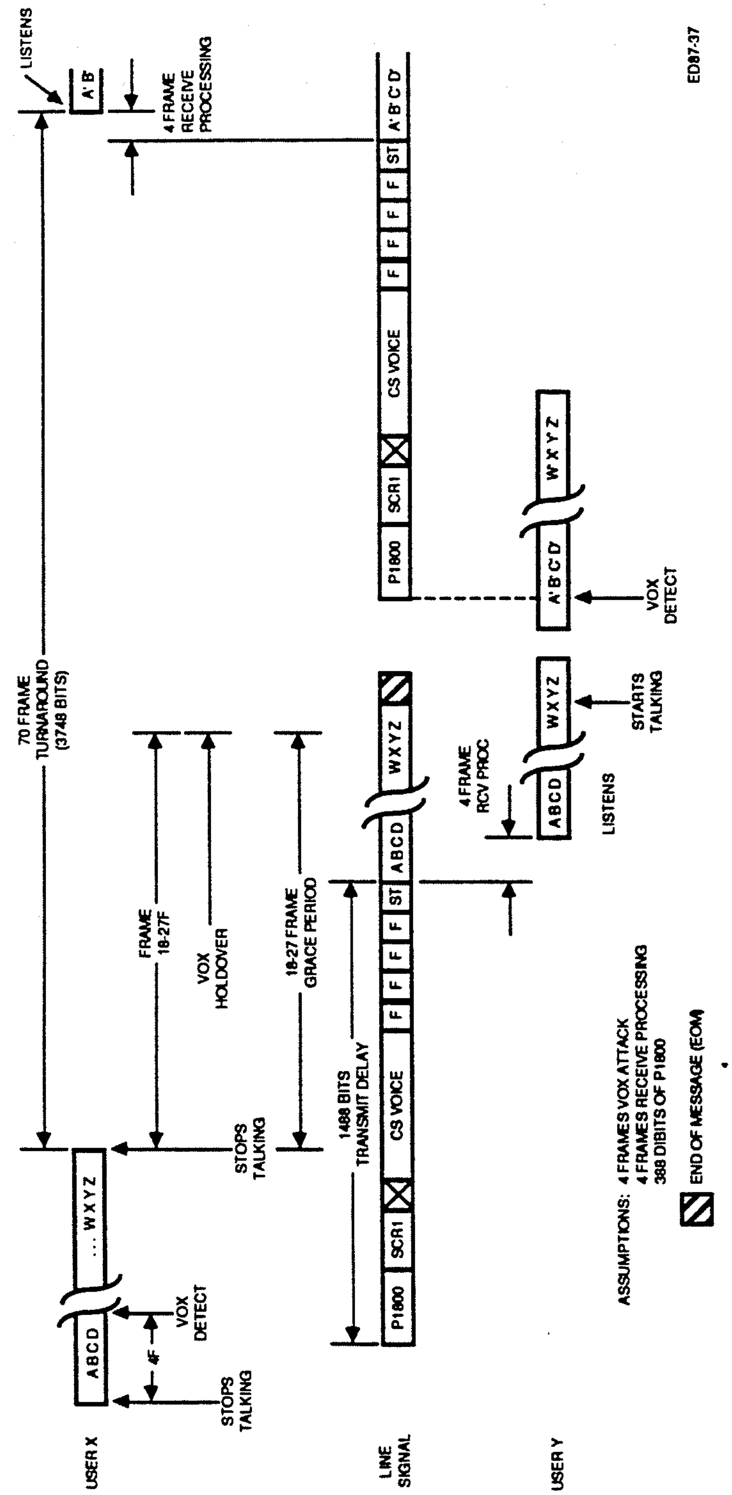


Figure 2-49. Half Duplex Turnaround Timeline

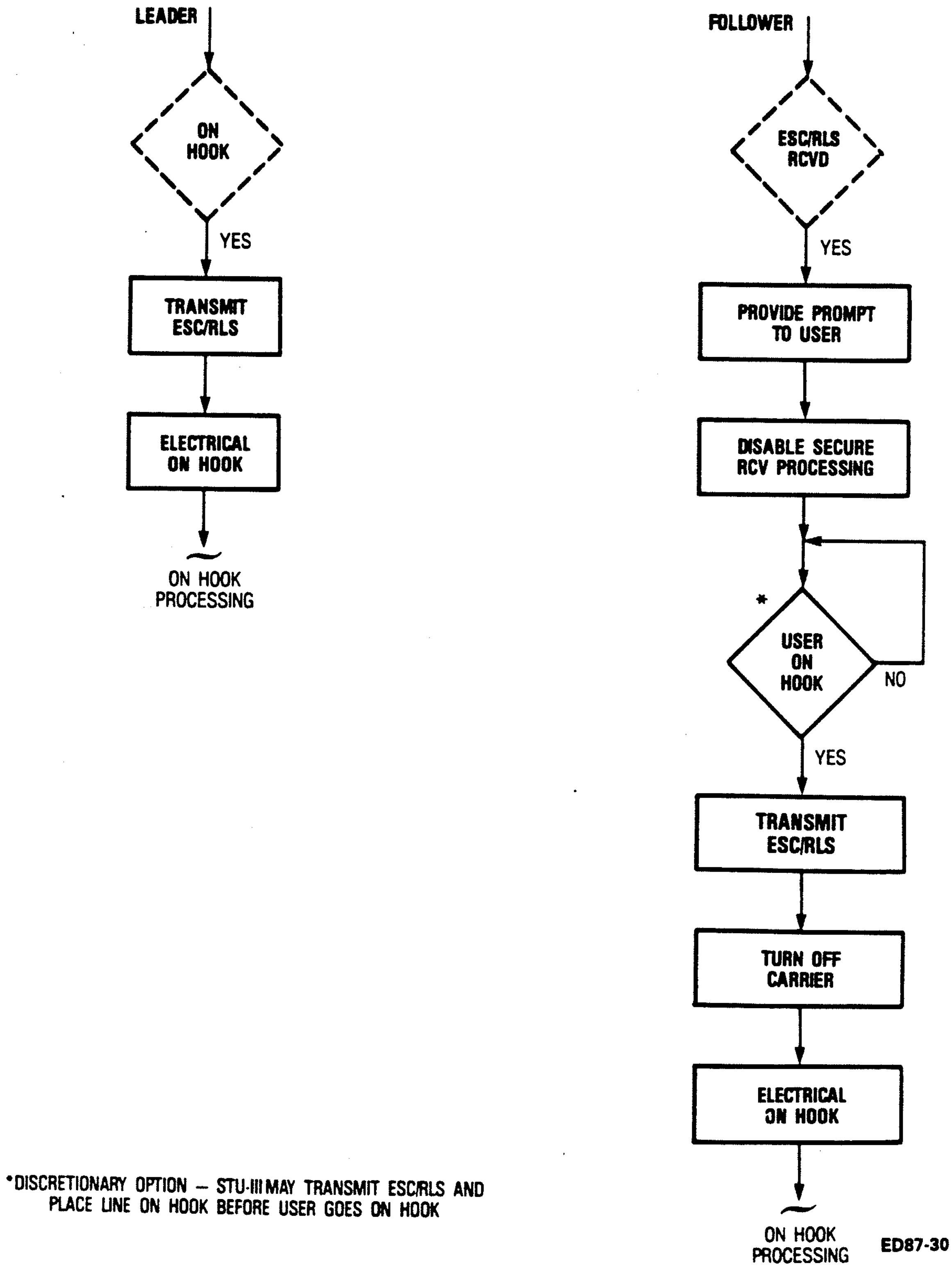


Figure 2-41. Full Duplex Release Processing

the time from VOX detection of a speech utterance until the first encrypted speech frame is transmitted) is equal to the length of the half duplex preamble and shall be less than 635 ms. The terminal shall have an 18-27 frame holdover on the voice transmission (i.e., when the VOX detects the absence of voice, the terminal shall continue transmitting for 18-27 LPC voice frame times). All buffered or stored voice frames, which contain voice information, shall be transmitted; however, silence frames may be deleted to reduce the transmission delay. At the conclusion of the voice transmission, the terminal shall transmit an unencrypted EOM.

The half duplex voice turnaround time (i.e., time from when one user completes an utterance until that same user can hear an utterance from the other subscriber) shall be less than 1600 ms assuming no transmission delay. A timeline for the minimum half duplex turnaround is depicted in Figure 2-49.

2.2.2.3.2 Half Duplex Secure Data; The STU-III will be capable of transmitting half duplex synchronous data securely at 2400 bps. It is intended that any vendor's Type I or Type II STU-III be interoperable with any other STU-III in the interoperable half duplex data mode.

The half duplex secure data mode shall be similar to the full duplex data mode except that data must be available for transmission, as defined in FSVS-220, before the STU-III can initiate data transmission when the user has selected the data mode. When the STU-III determines that data is available and the transmission line is available (i.e., no incoming signal), it shall send P1800, 3202, SCR1, SOM and CS (data) followed by at least four frames of Filler, Start and encrypted data traffic. The STU-III shall control the data flow such that the first bit of encrypted traffic shall correspond to the first bit of plaintext data available to the STU-III. When data is no longer available, the STU-III will complete the transmission of all available data and then transmit an unencrypted EOM followed by dropping of modem carrier within 50 ms.

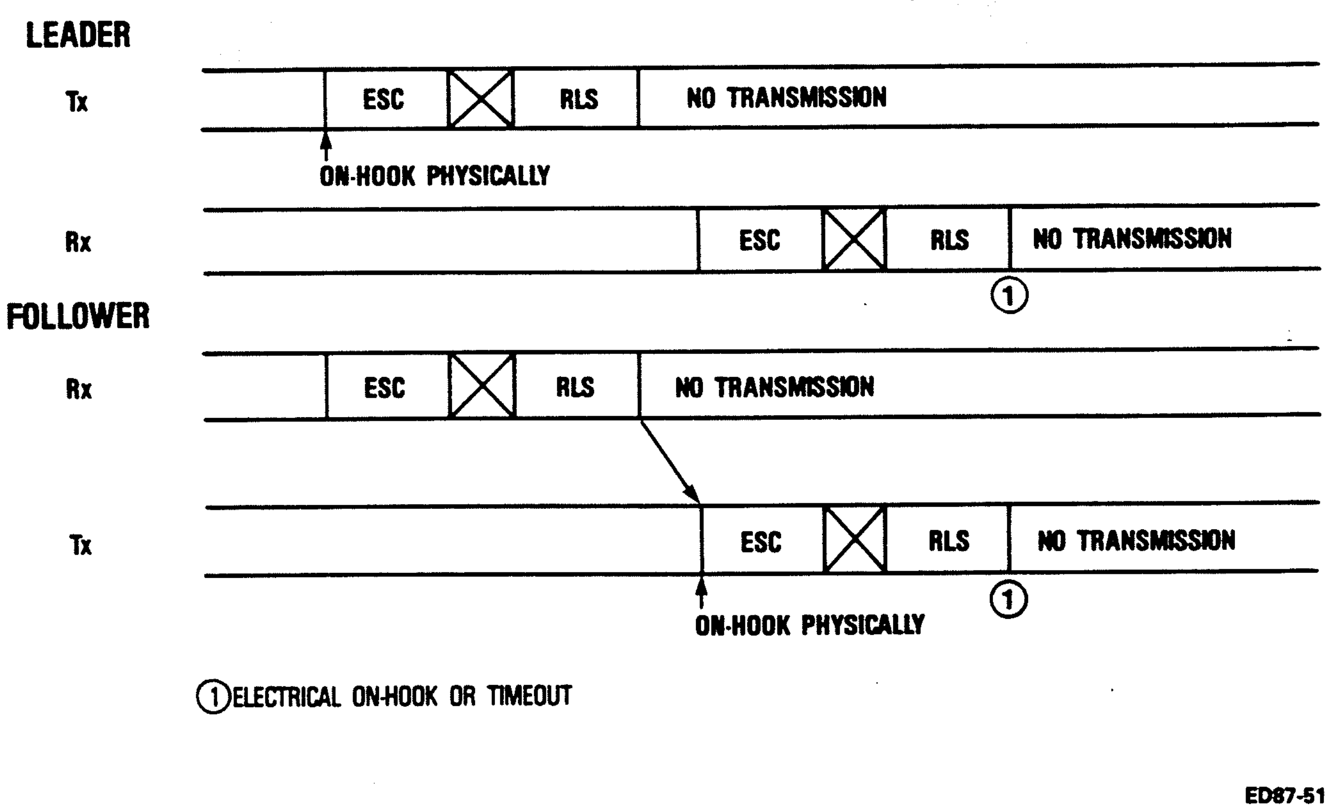


Figure 2-42. Full Duplex Release Sequence Signaling Diagram

message upon completion of RCC processing or upon receipt of a CS message, which ever occurs last, followed either by EOM or by traffic as determined by the status of the VOX (voice mode) or data device (data mode).

In order to send a CS message or secure traffic, the transmitting terminal shall verify that the transmission link has been idle for a minimum of 35 ms and shall then send P1800, 3202, SCR1 (32 dibits), SOM and the appropriate CS message followed by a minimum of four frames of Filler, Start, and secure traffic as described in the subsequent paragraphs. Following the transmission of all traffic, an unencrypted EOM shall be transmitted. In the half duplex traffic modes, the transmitting terminal shall remove modem carrier from the line within 50 ms after the transmission of the unencrypted EOM. Modem carrier must be removed from the line for a minimum of 35 ms.

A terminal which is not transmitting shall monitor the received line for the P1800 sequence. Upon detection of P1800, the receiving terminal shall process the received signal in accordance with the Signaling Plan. A terminal which is unable to process the received signal in accordance with the Signaling Plan shall monitor the line for loss of carrier. When loss of carrier is detected, the receiving terminal may enter the Failed Call sequence, or resume normal operation for processing half duplex traffic.

2.2.2.3.1 <u>Half Duplex Secure Voice</u>; The STU-III shall be capable of digitizing speech at a rate that can be transmitted half duplex at 2400 bps. Each STU-III will set the alternating 1/0 sync bit of the first speech frame of each half duplex transmission, to a "0".

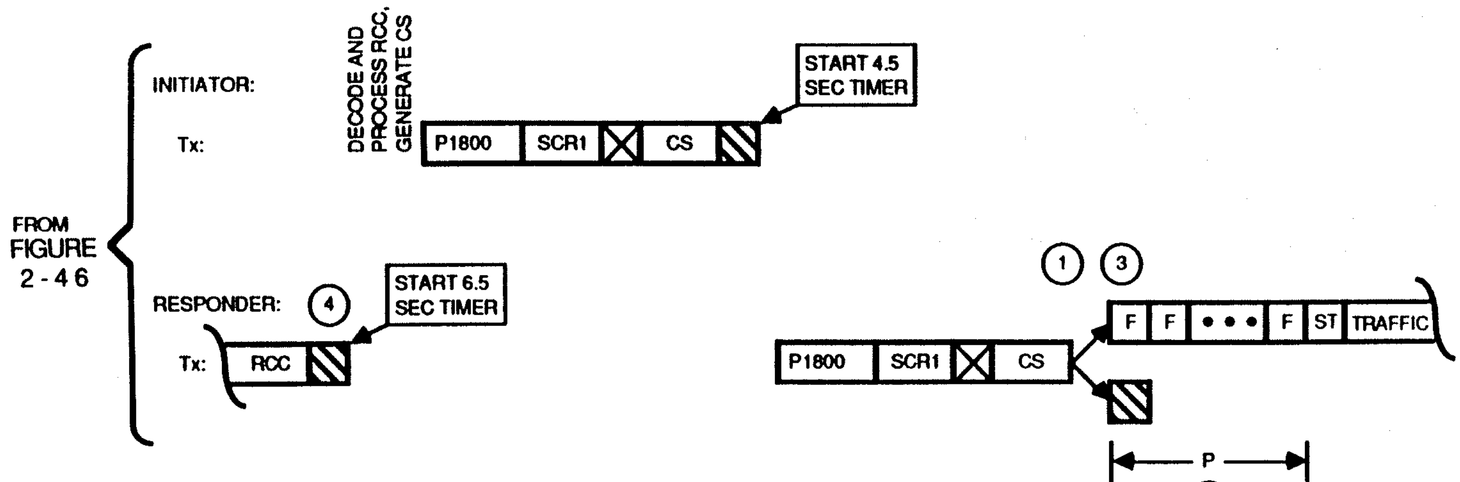
The half duplex secure voice cryptosync transmission shall be initiated by a voice operated switch (VOX) in the STU-III which has an attack time of four (or fewer) LPC-10 frames. The terminal will store the four (or fewer) voice frames resulting from the VOX determination as well as all additional LPC frames from the LPC analyzer which are produced while the terminal is transmitting the CS Voice message prior to encrypted traffic. The transmit delay time (i.e., end terminal to positively detect loss of carrier. The STU-III shall incorporate the timeouts shown in Table 2-3 when waiting for a message from the far end terminal. Table 2-3 defines the conditions and results of the specified timeouts for HDX operation. Timeout processing shall be as specified for FDX operation in Section 2.2.1.

The STU-III will support Plain Old Telephone Service (POTS) independent of the full/half duplex mode selected, as defined in Section 2.1. The unique half duplex operation, as defined in this section, is described in four major segments. Section 2.2.2.1 describes the initial call and modem training and the variable exchange phase is discussed in Section 2.2.2.2. The crypto synchronization and secure traffic descriptions have been combined in Section 2.2.2.3. Section 2.2.2.4 concludes with a discussion of the half duplex call interruption processing.

2.2.2.1 Half Duplex Initial Call/Modem Training

Once the analog clear call is established, the first user to depress the secure button will initiate the secure half duplex call sequence provided that the half duplex mode has been selected by either or both users. As described for full duplex operation, the terminal that initiates the secure signaling will assume the "initiator" role and the other terminal will assume the "responder" role. Figure 2-43 provides a state diagram for the initial call set-up and modem training. In the half duplex mode, the initiator will initially transmit a Pseudo 1800 Hz (P1800). For the responder, detection of 2100 Hz will indicate full duplex and the detection of Pseudo 1800 Hz (P1800) will establish the call as half duplex. The timeline for the half duplex initial call setup and modem training is shown in Figure 2-44.

Upon initiation of the secure half duplex call setup by the user, the initiator will check the line for detection of 2100 Hz or 1800 Hz carrier to reduce the possibility of a glare condition. In the absence of either signal, the STU-III will transmit



NOTES:

1. CS IS FOLLOWED BY EITHER EOM, OR FILLER/SOM/TRAFFIC DEPENDING ON THE STATE OF RESPONDER'S VOX (VOICE MODE) OR DATA AVAILABILITY (DATA MODE)
2. FOR SECURE VOICE P = 4,
   FOR SECURE DATA P ≥ 4.
3. SECURE TRAFFIC MODE ENABLED AFTER RECEPTION OF CS.
4. EOM:

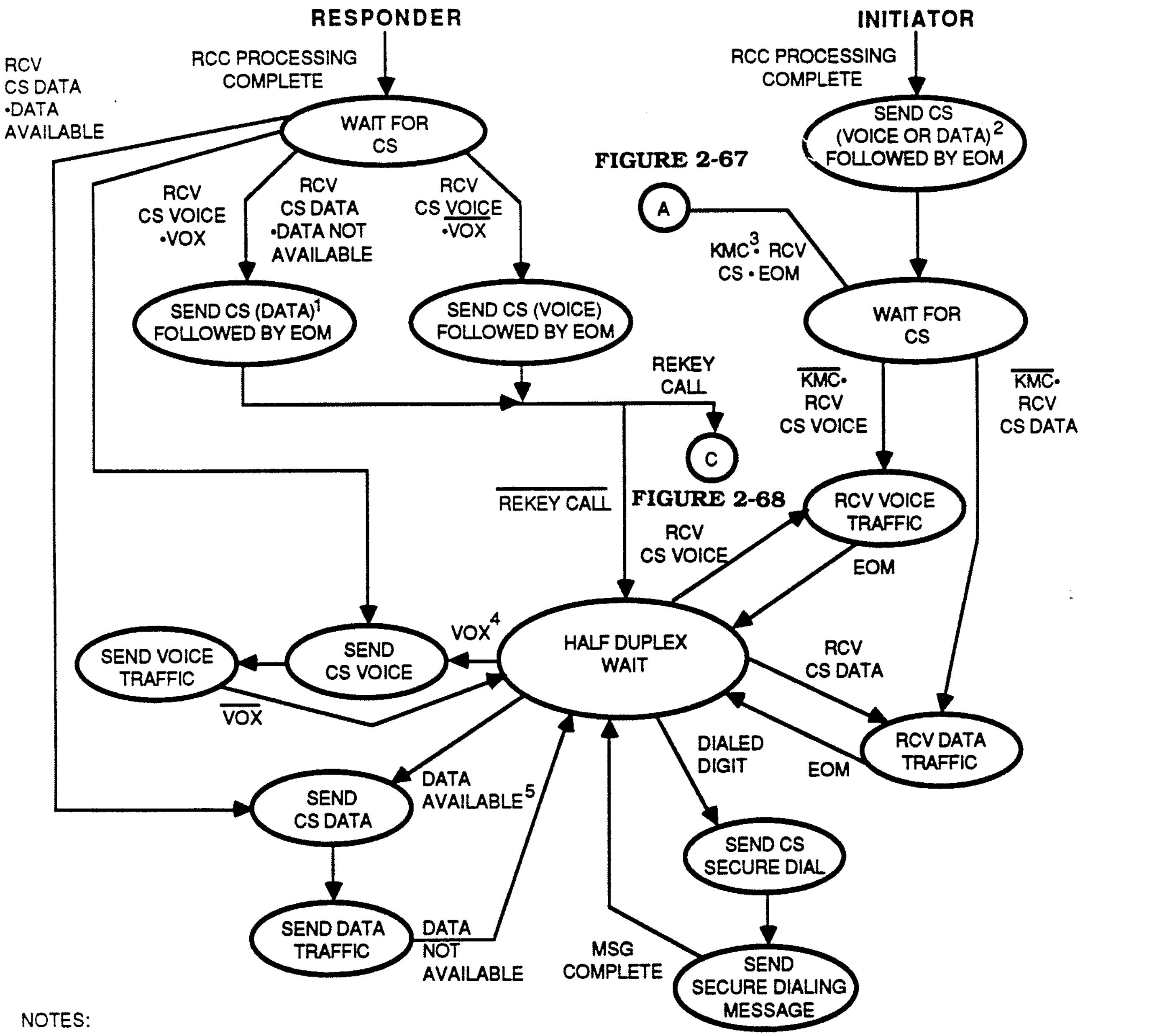
ED87-36

Figure 2-48. Half Duplex Cryptosync and Traffic Signaling Diagram

Table 2-3. Half Duplex Signaling Timeouts

The appropriate terminal, as indicated in column A, shall set a timer during selected points in the call/call set-up as indicated in B. The timer setting is defined in C. If the timeout is exceeded before the expected message in D is detected, the terminal shall enter the signaling sequence in E.

A	B	C	D	E
Terminal Setting Timer	**Message Transmitted Starts Timer**	**Timer Value**	**Expected Message Response**	**Response to Timeout**
Initiator	Final bit of EOM of CAP/SV	2.5 ± .6 sec	P1800	Failed Call
Responder	Final bit of EOM of TC	2.5 ± .6 sec	P1800	Failed Call
Initiator	Final bit of EOM of RCC	2.5 ± .6 sec	P1800	Failed Call
Responder	Final bit of EOM of RCC	6.5 ± .6 sec	P1800	Failed Call
Initiator	Final bit of EOM of CS	4.5 ± .6 sec	P1800	Failed Call



NOTES:

1. ON A REKEY CALL, THE STU-III ACTS AS RESPONDER AND SHALL FOLLOW THIS PATH AND SEND CS HALF RATE DATA (HDX).
2. ON A REKEY CALL, THE KMC ACTS AS INITIATOR AND SHALL SEND CS HALF RATE DATA (HDX) FOLLOWED BY EOM.
3. "KMC" INDICATES THE PATH FOLLOWED BY THE KMC ON A REKEY CALL AFTER RECEIVING THE CS HALF RATE DATA (HDX) FOLLOWED BY EOM FROM THE STU-III.
4. THIS TRANSITION SHALL OCCUR ONLY IF THE STU-III IS IN THE VOICE MODE.
5. THIS TRANSITION SHALL OCCUR ONLY IF THE STU-III IS IN THE DATA MODE.
6. ON-HOOK DURING ANY STATE WILL CAUSE A TRANSITION TO RELEASE.
7. ALARM OR FAILURE CONDITION, WILL CAUSE A TERMINATE OR A TRANSITION TO FAILED CALL.
8. ACTIVATION OF NON-SECURE OR RECEIPT OF ABORT DURING ANY STATE WILL CAUSE A TRANSITION TO ABORT STATE.

ED87-35

Figure 2-47. Half Duplex Cryptosync/Traffic Sequence Flow Diagram

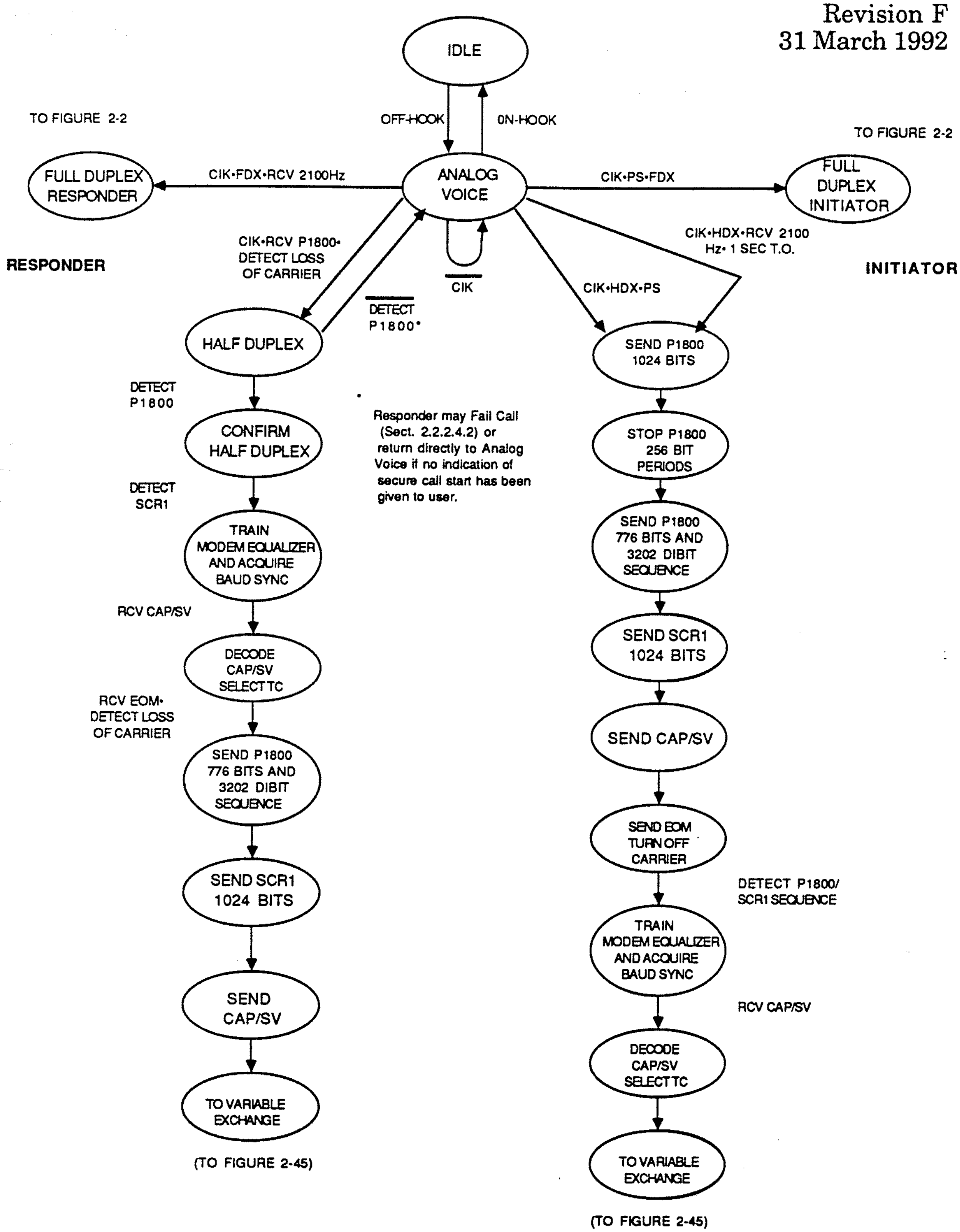


Figure 2-43. Half Duplex Initial Call / Modem Training Sequence Flow Diagram

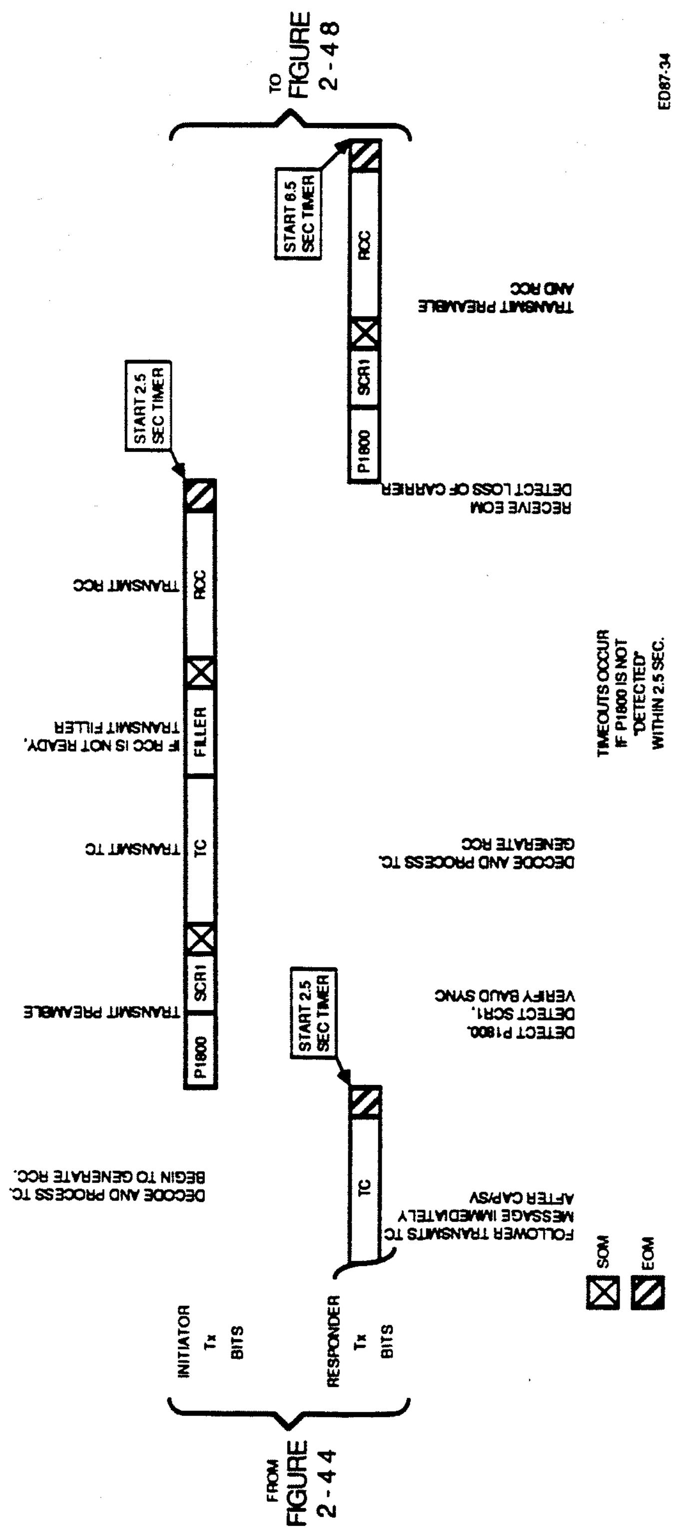


Figure 2-46. Half Duplex Variable Exchange Signaling Diagram

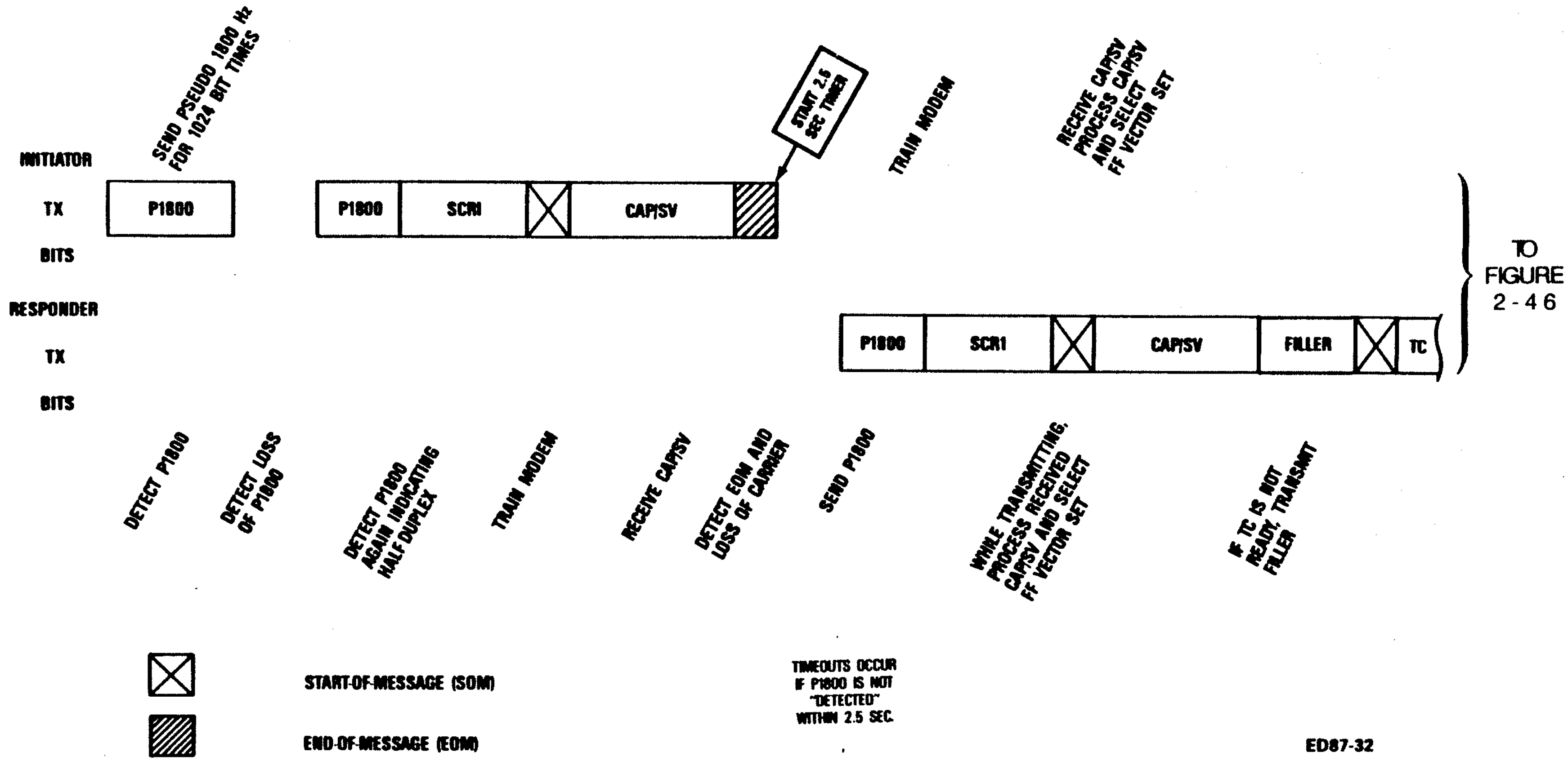


Figure 2-44. Half Duplex Initial Call/Modem Training Signaling Diagram

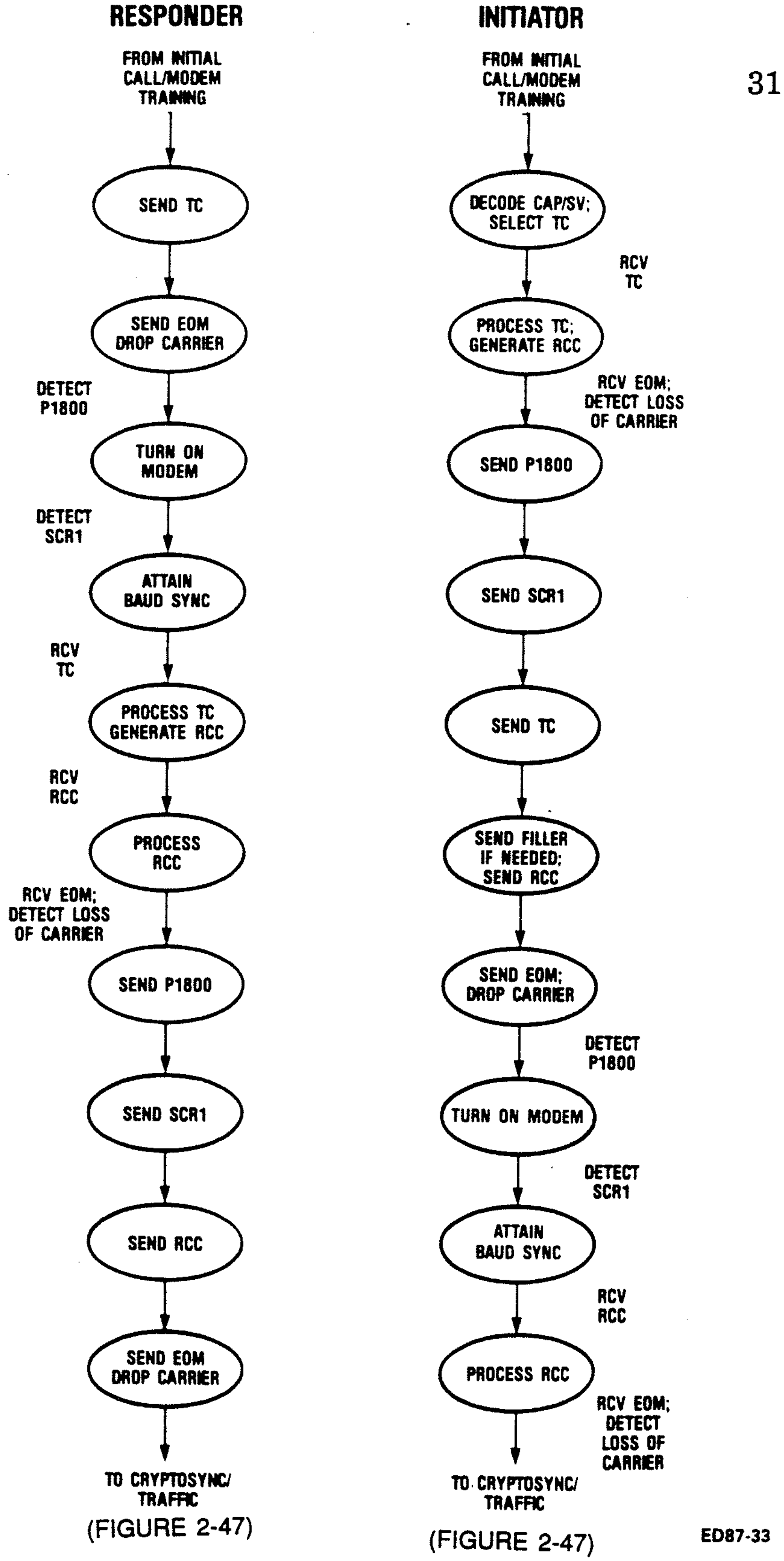


Figure 2-45. Half Duplex Variable Exchange Sequence Flow Diagram

P1800 for 1,024 bits (512 dibits). The initiator will then turn off carrier for 256 bit times (128 dibits), and then transmit P1800 for 776 bits (388 dibits), followed immediately by a 3202 transition dibit sequence. The responder will detect P1800 and determine that the half duplex call setup is being established. The short gap in P1800 will be used to distinguish a half duplex initiator from a full duplex responder, and also to differentiate between STU-II and STU-III signaling. The initiator will then transmit SCR1 for 1,024 bits (512 dibits) using the GPC scrambler to allow the responder to train its modem equalizer. The initiator will then transmit its Capability/Status Vector (CAP/SV) message followed by an End-of-Message (EOM) pattern and drop modem carrier within 50 ms.

The responder will receive the CAP/SV message, compare the contents with its own capabilities and FIREFLY status, and determine the COMSEC mode and FIREFLY vector set for the call. Upon detecting EOM and loss of carrier for at least 35 ms, the responder will transmit P1800, the 3202 transition dibit sequence, SCR1 for 1,024 bits (512 dibits) using the GPA scrambler, and the CAP/SV message. The initiator will detect the P1800 carrier and look for the transition to SCR1. The initiator will detect the transition to SCR1 and train its modem equalizer for 400 ms. The initiator will then receive the CAP/SV message, compare the contents with its own, and determine the COMSEC mode and FIREFLY vector set for the call.

2.2.2.2 Half Duplex Variable Exchange

During the second phase of the half duplex call setup, the Terminal Cipher (TC) and the Random Component Cipher (RCC) messages are exchanged between the two STU-IIIs. As a result of the CAP/SV messages that were exchanged during the Initial Call/Modem Training sequence, each terminal shall independently select the most recent version of the highest common class of FIREFLY keying material. The state diagram and timeline for the variable exchange are depicted in Figures 2-45 and 2-46, respectively.

Exchange of Terminal Cipher (TC). If the responder has received the CAP/SV message and determined the appropriate TC, it will continue by transmitting the TC message immediately following the CAP/SV that, in turn, will be followed by an EOM. The responder may transmit Filler until the TC is ready for transmission. The initiator will receive TC, decode it, and determine the classification for the call. Upon receiving EOM and detecting loss of carrier for at least 35 ms, the initiator will transmit P1800, followed by 3202, SCR1 (32 dibits), SOM, its TC message, and Filler. Transmission of Filler is optionally included when necessary to allow sufficient time for either terminal to generate the next message without requiring the retransmission of the preamble.

Exchange of Random Component Cipher (RCC). Each terminal shall use the decoded information from the TC message to generate and encode the RCC message. The initiator will continue to transmit FILLER until the RCC is ready for transmission at which time the RCC will be transmitted followed by EOM and the dropping of the modem carrier within 50 ms. When the responder detects EOM and loss of carrier for at least 35 ms, and the RCC has been prepared for transmission, the responder will transmit P1800, 3202, SCR1 (32 dibits), SOM, and the RCC message followed by EOM and the dropping of carrier. Upon receipt of RCC, each terminal will decode the message and prepare for synchronization and secure traffic.

2.2.2.3 Half Duplex Crypto Synchronization/Secure Traffic

The half duplex scheme adopted for the STU-III design requires a new crypto synchronization each time the link is used for a secure transmission. Either terminal may transmit one of several cryptosync messages (e.g., CS Voice, CS Data, CS Half Rate, CS Secure Dial) to initiate a secure traffic transmission as shown in the state diagram and timeline of Figure 2-47 and Figure 2-48, respectively. Neither the initiator nor the responder may transmit traffic before receiving a CS message. The initiator shall send a CS message followed by an EOM upon completion of RCC processing. The responder shall send a CS